

Mit „Sicherheit“ zum Polizeistaat? FAQ zum (vielleicht bald) neuen Polizeirecht in Sachsen

Sachsens Minderheitsregierung will das Polizeirecht umfassend novellieren. Wir als Fraktion Die Linke haben große und zahlreiche Bedenken gegen die geplanten neuen Überwachungsbefugnisse und stehen damit nicht allein. Dem Entwurf samt Taser-Waffen, sogenannter Quellen-Telekommunikationsüberwachung (TKÜ) zur Chatüberprüfung und Künstlicher Intelligenz im „Palantir“-Stil werden wir nicht zustimmen. Hier erklären wir ausführlich, worum es geht und woran wir uns stören.

Wer nicht lesen will: Die Fraktion Die Linke hat in Dresden, Zwickau und Leipzig mehrere Podien zur Polizeirechtsnovelle durchgeführt. Die Aufzeichnung aus Leipzig gibt's [hier zum Nachhören](#).

Das Gesetzesvorhaben – 1: Wozu dient der Gesetzentwurf?

Die Staatsregierung hat dem Parlament am 25. Februar 2026 den Entwurf für ein „Gesetz zur Änderung polizeirechtlicher Vorschriften“ vorgelegt ([Drucksache 8/6142](#)). Darin vorgesehen sind umfangreiche Änderungen und Erweiterungen am Sächsischen Polizeivollzugsdienstgesetz (SächsPVDG). Das SächsPVDG regelt, welche Aufgaben die Landespolizei hat, welche Mittel und Methoden sie unter welchen Voraussetzungen anwenden darf, welche Daten sie erheben und speichern kann. Stark verkürzt gesagt: Es geht um die zentralen „Spielregeln“ der Polizei im Freistaat. Sie sollen jetzt in sehr kurzer Zeit, bis Mitte 2026, ganz umfassend erneuert werden.

Das Gesetzesvorhaben – 2: Warum muss das Gesetz geändert werden?

Es gibt einen „harten“ Grund, warum eine Novellierung erfolgen muss: ein Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024 ([Aktenzeichen Vf. 91-II-19](#)) gegen das bisherige Gesetz von 2019. Dagegen hatten Landtagsabgeordnete der Linken und der Grünen gemeinsam geklagt, weil nach unserer Auffassung die Schwellen für etliche Polizei-Befugnisse, darunter heimliche Überwachungsmaßnahmen, unklar waren und zu niedrig lagen. Vereinfacht gesagt: Die Polizei darf bisher zu früh schon zu viel unternehmen, zum Beispiel Handys abhören, Personen observieren oder auch V-Leute einsetzen.

Das Gericht hat uns Anfang 2024 in vielen Punkten Recht gegeben und geurteilt, dass etliche Befugnisse nicht mit der Sächsischen Verfassung vereinbar sind. Das Gericht hat außerdem „Auflagen“ verhängt: Die verfassungswidrigen Befugnisse dürfen nur noch nach strengen Vorhaben angewandt werden, und zwar maximal bis zum 30. Juni 2026. Werden die verfassungswidrigen Befugnisse bis dahin nicht ausgebessert, fallen sie weg. Die sächsische Polizei würde damit in vielen Bereichen praktisch handlungsunfähig werden.

Das Gesetzesvorhaben – 3: Wo liegt jetzt das Problem?

Problem Nummer 1: Noch 2024, kurz nach der letzten Landtagswahl, hatten wir als Fraktion Die Linke mit einem Antrag die Staatsregierung aufgefordert, das Urteil schnellstmöglich umzusetzen ([Drucksache 8/713](#)). Stattdessen ist erst einmal gar nichts passiert. Der jetzt vorliegende Gesetzentwurf kommt rund zwei Jahre nach dem Verfassungsgerichts-Urteil, dem man buchstäblich auf den letzten Drücker doch noch nachkommen will.

Aber der Gesetzentwurf bringt Problem Nummer 2 mit: Plötzlich stehen Taser-Waffen, die sogenannte Quellen-TKÜ zur Chatüberwachung und Künstliche Intelligenz im „Palantir“-Stil im Raum. Diese Neuerungen haben mit dem Urteil nichts zu tun, sondern sind politisch motivierte Ziele der CDU-SPD-Koalition, mit klarer Färbung des stockkonservativen Innenministeriums. Durch die umfangreichen Zusatzwünsche handelt sich um eines der komplexesten Rechtsetzungsvorhaben dieser Wahlperiode. Und durch die Frist des Verfassungsgerichts-Urteils muss über all das bis zum 30. Juni 2026 entschieden sein – statt dem Parlament die nötige Zeit zu geben, sich mit allen Details auseinanderzusetzen, die sich etwa aus neuen KI-Technologien ergeben. Wir sehen die akute Gefahr, dass demnächst im Hauruck-Verfahren ein Gesetz verabschiedet wird, das (erneut) nicht mit den Grund- und Freiheitsrechten in Einklang steht.

Das Gesetzesvorhaben – 4: Wie hat sich das Parlament mit dem Gesetzentwurf auseinandergesetzt?

Von den Plänen haben wir erstmals am 2. Oktober 2025 erfahren. Damals wurde uns eine frühe Fassung (der sogenannte Referentenentwurf aus dem Innenministerium) vorgelegt. Wir haben daraufhin von unserer Möglichkeit Gebrauch gemacht, im Rahmen des sächsischen Konsultationsverfahrens, mit dem die Minderheitsregierung ihre Mehrheitschancen auslotet, eine umfangreiche fachpolitische Stellungnahme (38 Seiten) vorzulegen.

Der „echte“ Gesetzentwurf (mit unserer und weiteren Stellungnahmen als Anhang) datiert vom 25. Februar 2026 ([Drucksache 8/6142](#)). Einiges hat sich darin geändert, aber unsere kritischen Anmerkungen sind im Großen und Ganzen verhallt, ebenso wie beispielsweise die umfangreichen Bedenken der Sächsischen Datenschutz- und Transparenzbeauftragten. Am 27. März 2026 fand im Innenausschuss eine öffentliche Anhörung ([Protokoll](#), [Videoaufzeichnung](#)) mit elf Sachkundigen statt, die mit den Ausschussmitgliedern mehr als fünf Stunden lang kontrovers über den Entwurf diskutierten.

Das Gesetzesvorhaben – 5: Wie geht es weiter und welche Chancen hat der Gesetzentwurf?

Da in Sachsen eine Minderheitskoalition regiert, die keine eigene Landtagsmehrheit hat, braucht es für den Beschluss zusätzliche Stimmen aus der Opposition. Die kommen entweder von Linken und Grünen oder aber vom BSW. Da wir als Linke wie auch die Grünen umfangreiche Kritik am Entwurf geäußert haben, der kaum begegnet wurde, kommt nur noch das BSW in Frage. Dass die Koalition auf die BSW-Fraktion setzt, war

schon frühzeitig zu erahnen, denn deren Stellungnahme zum alten Referentenentwurf ist mit dreieinhalb Seiten eher überschaubar geblieben. Was aktuell noch aussteht, ist eine abschließende (nicht-öffentliche) Behandlung im Innenausschuss. Anschließend wird der Gesetzentwurf im Plenum zur Abstimmung gestellt. Das wird aller Voraussicht nach am 24. Juni 2026 passieren.

Das Gesetzesvorhaben – 6: Wird die Fraktion Die Linke den Gesetzentwurf ablehnen?

Ja, weil wir Prinzipien haben und unsere Bedenken sehr schwer wiegen. Darüber hätten wir uns mit CDU und SPD, so wie das unter demokratischen Fraktionen üblich ist, auch näher ausgetauscht, um Kompromisse zu suchen, mit denen die Grund- und Freiheitsrechte gewahrt bleiben. Zu Verhandlungen wurden wir aber erst gar nicht gebeten.

Das Gesetzesvorhaben – 7: Kann der Gesetzentwurf noch scheitern?

Theoretisch ja, falls das BSW „abspringt“, wofür wir keine Anzeichen sehen. Es würde dann eine Situation eintreten, die es so noch nie gegeben hat: Die Koalition müsste sich entscheiden, ob sie den Gesetzentwurf trotzdem zur Abstimmung stellt, auf die Gefahr hin, erstmals in Sachsen eine Mehrheit mit der AfD zu bilden. Stellt sie den Gesetzentwurf nicht zur Abstimmung, würde die Frist des Verfassungsgerichts-Urteils gerissen.

Als Alternative liegt neuerdings ein paralleler Gesetzentwurf der Grünen vor, der sich im Wesentlichen darauf beschränken würde, die Maßgaben des Urteils umzusetzen. Es wäre wiederum ein Novum, wenn die regierungstragenden Fraktionen einem Oppositions-Gesetzentwurf zustimmen würden, obwohl sie eine eigene Vorlage vertreten. Es könnte also durchaus noch einmal spannend werden auf den letzten Metern.

Die neuen Befugnisse – 8: Braucht die sächsische Polizei neue Befugnisse?

Das klingt vielleicht überraschend, aber auch aus linker Sicht ist die Antwort: Ja, die Polizei braucht moderne Befugnisse auf der Höhe der Zeit, um mit gesellschaftlichen Entwicklungen Schritt halten und auch verletzliche soziale Gruppen besser schützen zu können. Ein Beispiel dafür sind Maßnahmen gegen häusliche Gewalt und Stalking. Hier hätten wir uns sogar noch weitergehende Lösungen vorstellen können, als sie der Gesetzentwurf vorsieht. Bei vielen weiteren Befugnissen, mit denen die sächsische Polizei jetzt ausgestattet werden soll, geht es aber um ganz andere Dinge. Dabei steht aus unserer Sicht leider nicht der Schutz von Betroffenen im Vordergrund, sondern eine allgemeine Aufrüstung der Polizei und eine zunehmende Macht über die Daten potenziell aller Bürgerinnen und Bürger – zu Lasten der Grund- und Freiheitsrechte.

Die neuen Befugnisse – 9: Soll die Polizei denn nicht Schritt halten können mit Kriminellen?

Das wird oft gesagt, wird aber dadurch nicht richtig. Im demokratischen Rechtsstaat soll und will die Polizei gar nicht „alles“ dürfen. Denn eine ihrer Kernaufgaben ist der Schutz der Rechte der Menschen, nicht der immer umfänglichere und tiefere Eingriff in diese

Rechte. Genau das passiert aber durch immer mehr Überwachungsinstrumente und Datenerhebungsbefugnisse, die oft zwangsläufig auch völlig Unbeteiligte betreffen. Polizeiliche Befugnisse müssen verhältnismäßig sein, dem widerspricht die Idee einer „Waffengleichheit“. Aus einer immer stärkeren Aufrüstung der Polizei folgt auch nicht automatisch mehr Sicherheit, sondern im Zweifel: Einschüchterung.

Es kommt noch ein anderer Aspekt hinzu, der oft übersehen wird. Im Polizeivollzugsdienstgesetz geht es nicht um die Verfolgung von Straftäterinnen und Straftätern, sondern um sogenannte Gefahrenabwehr. In dieser Rolle handelt die Polizei im Vorfeld von Straftaten, bevor irgendetwas passiert ist. Dazu passt es nicht, wenn laut dem Gesetzentwurf genau in diesem Bereich, in dem oft nicht mehr vorliegt als irgendein vager Verdacht oder eine hypothetische Prognose, die Polizei sogar schon „mehr“ tun darf als bei der Verfolgung von Straftaten.

Die neuen Befugnisse – 10: Wie schätzt die Linksfraktion die neuen Befugnisse insgesamt ein?

Wir sehen das im Einzelnen differenziert und betonen gern: Nicht alles an dem Gesetzentwurf ist schlecht. Ein Beispiel: Die Polizei hortet Unmengen von Informationen in einer Art Datenbank, dem Polizeilichen Auskunftssystem, kurz PASS. Mit dem Gesetzentwurf wird dieser Bereich der sogenannten vorsorgenden Speicherung endlich umfassend geregelt: Was darf wie lange gespeichert werden, wann ist es zu löschen? Es ist zu begrüßen, wenn es für diese Standardpraxis, die aus der Polizeiarbeit nicht wegzudenken ist, endlich eine nachvollziehbare Regelung gibt.

In anderen Fällen werden allerdings Regelungen geschaffen, die weniger gut nachzuvollziehen sind und mit denen auch eine völlig neue Praxis der Polizei einhergehen wird: so die Ausweitung des Taser-Einsatzes, die Drohnenabwehr, die Quellen-Telekommunikationsüberwachung und die Künstliche Intelligenz.

Die neuen Befugnisse – 11: Was ist das Problem mit dem Taser?

Taser, offiziell „Distanzelektroimpulsgeräte“ (DEIG) genannt, sind Elektroschock-Pistolen, die Menschen einen Stromschlag versetzen und sie damit angriffsunfähig machen. Solche Geräte werden in Sachsen bereits genutzt, allerdings nur durch das Spezialeinsatzkommando (SEK). Das Innenministerium will den Taser für die gesamte Polizei freigeben, auch für den ganz normalen Streifendienst. Argumentiert wird mit der angeblichen Deeskalationswirkung und dass so die Anwendung der Schusswaffe vermieden werden könnte. Das klingt beinahe verlockend, überzeugt uns aber aus mehreren Gründen nicht.

Keineswegs wird der Taser ein Ersatz für die Schusswaffe sein. In der Praxis wird die Polizei beides tragen und im Zweifel beides einsetzen. Auch Taser können schwere Verletzungen verursachen, erhöhte gesundheitliche Gefahren drohen insbesondere Menschen mit Vorerkrankungen, unter Medikamenteneinfluss, Schwangeren und Kindern. Das lässt sich nicht immer vorab erkennen. Daher lässt es sich auch nicht vermeiden, verletzliche Personen zu treffen.

In mehreren anderen Bundesländern wurden Taser schon eingeführt. Aus den durchgeführten Studien ergibt sich kein Beleg dafür, dass diese Waffen zur Deeskalation führen. Sie sorgen aus unserer Sicht eher für Einschüchterung. Für das „Abdrücken“ des Tasers gelten (anders als für Schusswaffen) auch keine erhöhten Voraussetzungen, rechtlich gesehen sind sie zum Beispiel dem Schlagstock gleichgestellt und werden genauso „locker“ sitzen.

Die sächsischen Erfahrungen sind keineswegs vielversprechend, wie unsere Kleine Anfrage ([Drucksache 8/5074](#)) zeigt. Taser sind bei jedem SEK-Einsatz dabei, wurden in den letzten drei Jahren aber insgesamt nur sechs Mal benutzt. Selbst in besonders „robusten“ Situationen ist der Einsatzbedarf offenbar nicht besonders groß.

Es gibt außerdem ein Detail, das krasse Folgen haben könnte: Das Wort „Taser“ steht nicht im Gesetz, und das ist ein Problem. Dort ist die Rede von „Vorrichtungen für den Abschuss besonderer Formen von Projektilen, die darauf ausgerichtet sind, die betroffene Person zu überwältigen, ohne sie dabei tödlich zu verletzen.“ Diese Definition umfasst auch Gummi- und Plastikgeschosse. Sie dürften künftig zum Beispiel gegen Versammlungen eingesetzt werden.

Die neuen Befugnisse – 12: Was ist das Problem mit der Drohnenabwehr?

Die sächsische Polizei betreibt bereits eine Drohnenabwehr-Einheit, [wir haben aktuelle Einsatzzahlen erfragt](#). Die Drohnenabwehr dient beispielsweise dazu, Großveranstaltungen vor gefährlichen Überflügen und Einrichtungen der sogenannten Kritischen Infrastruktur vor möglichen Ausspähungen zu schützen. Bisher stützt sich die Polizei dabei auf ihre allgemeine Gefahrenabwehr-Aufgabe, eine sogenannte Generalklausel. Mit der Gesetzesänderung wird erstmals eine auf die Drohnenabwehr zugeschnittene Regelung geschaffen. Sie erlaubt es zum einen, Drohnen zu detektieren, und zum anderen, sie mit technischen Mitteln abzufangen. Angesichts des Schadenspotenzials unkontrollierter Drohnenflüge und des Missbrauchsmöglichkeiten für Angriffe ist das nachvollziehbar. Aber die geplante Umsetzung überzeugt uns nicht.

Der Gesetzentwurf lässt offen, wie genau die Abwehr ablaufen soll. Die Rede ist von „technischen Mitteln“ und von „physischen Mitteln“. In der Begründung tauchen sogar Laser auf – die als Waffe angesehen werden könnten, was der Gesetzestext aber nicht vorsieht. So oder so: Der Gesetzgeber, also das Parlament, muss wissen, worüber er wirklich beschließt. An dieser Stelle halten wir die Regelung für zu unbestimmt.

Die Drohnenabwehr soll ausdrücklich auch dann durchgeführt werden dürfen, „wenn Dritte unvermeidbar betroffen werden“, also wenn Personen etwa durch herabstürzende Teile verletzt werden. Die dem Gesetz zufolge bei jeder Maßnahme vorzunehmende Prüfung der Verhältnismäßigkeit wird dadurch umgangen. Paradoxe Folge: Gerade durch eine erfolgreiche Drohnenabwehr könnten Gefahren eintreten, die eigentlich verhindert werden sollen.

Es fehlt zudem eine klare Verantwortlichkeit. Aus Sicht der Fraktion Die Linke wäre es nötig, die Anwendung der Drohnenabwehr abhängig zu machen von der Anordnung durch eine Einsatz- oder Behördenleitung. Weil das nicht vorgesehen ist, werden Fälle des Falles „einfache“ Beamtinnen und Beamte den Kopf hinhalten müssen.

Die neuen Befugnisse – 13. Was ist das Problem mit der Quellen-Telekommunikationsüberwachung?

Schon bisher darf die sächsische Polizei unter bestimmten Voraussetzungen Telefone abhören und SMS mitlesen: die so genannte Telekommunikationsüberwachung (TKÜ), bei der die Provider den Datenverkehr für die Polizei ausleiten. Diese Methode geht heute oft ins Leere, denn die Regel sind verschlüsselte Messenger-Dienste, über die auch telefoniert werden kann; mit den ausgeleiteten Daten kann die Polizei nichts anfangen. Die Quellen-TKÜ geht daher buchstäblich an die Quelle“ und fängt die Daten auf den Geräten von Nutzerinnen und Nutzern ab, bevor der Kommunikationsinhalt verschlüsselt übertragen wird oder nachdem er übertragen wurde und wieder im „Klartext“ (oder Klarton) vorliegt. Es mag Fälle geben, in denen die Polizei ein völlig nachvollziehbares Interesse daran hat, den Inhalt verschlüsselter Kommunikation zu kennen. Aber hier sehen wir grundlegende Probleme, die umfassender diskutiert werden müssen.

Die Quellen-TKÜ ist nicht nur einfach eine modernere Form des „normalen“ Abhörens, bei der in das grundrechtlich geschützte Fernmeldegeheimnis eingegriffen wird. Sondern es handelt sich um einen zusätzlichen Eingriff in die grundgesetzlich geschützte Vertraulichkeit und Integrität informationstechnischer Systeme. Aufgrund dieses vertieften Eingriffs müssten die Eingriffsschwellen höher liegen. Der Gesetzentwurf trägt dem nur unzureichend Rechnung.

In der Praxis heißt Quellen-TKÜ: Die Polizei muss das Kommunikationsgerät (zum Beispiel ein Handy) „hacken“. Das geschieht etwa durch die Anwendung des sogenannten Bundestrojaners oder durch andere Methoden, um mit dem Messenger-Dienst unbemerkt ein Polizeigerät zu koppeln, auf dem dann alles mitgelesen werden kann. Die Polizei hat dadurch ein Interesse daran, IT-Schwachstellen zu finden – aber nicht, um sie zum Schutz aller Bürgerinnen und Bürger zu schließen, sondern um sie bewusst geheim zu halten und bestehen zu lassen. Darin sehen wir ein Risiko, denn solche Schwachstellen lassen sich ebenso durch Kriminelle oder Geheimdienste ausnutzen.

Bisher und auch künftig nicht erlaubt ist die sogenannte Online-Durchsuchung. Aber technisch ist das weitgehend derselbe Vorgang wie die Quellen-TKÜ, nur dass über die „laufende Kommunikation“ hinaus auch ehemalige Kommunikation aus dem Chat-Archiv ausgelesen werden dürfte. Auch wenn solche Daten bei der Quellen-TKÜ nicht verwertet werden können, trifft der Gesetzentwurf keine Vorkehrungen, um zu verhindern, dass die Polizei sie trotzdem abgreift.

Die neuen Befugnisse – 14: Was ist das Problem mit der Künstlichen Intelligenz?

Für viele Menschen ist „Künstliche Intelligenz“ (KI) nicht mehr aus dem Alltag und auch dem Arbeitsleben wegzudenken. Das ist bei der Polizei nicht anders, in einigen Bereichen setzt sie bereits auf Software-Tools mit KI-Funktionalitäten, wie eine unserer aktuellen Kleinen Anfragen zeigt ([Drucksache 8/5075](#)). Keine Frage: Für solche automatisierten Assistenzsysteme gibt es sinnvolle Anwendungsbereiche – man denke an die besonders belastende Prüfung von Foto- und Videomaterial auf mögliche Missbrauchsdarstellungen. Der Gesetzentwurf geht aber einen großen Schritt in eine

ganz andere Richtung. Denn erstmals soll es der Polizei ermöglicht werden, mächtige KI-Systemen „live“ für Überwachungsaufgaben einzusetzen.

Im Einzelnen sollen folgende KI-Befugnisse geschaffen werden, gegen die wir aus verschiedenen Gründen große Vorbehalte hegen:

- KI-Videoüberwachung zur automatischen Muster-Erkennung, Markierung, Nachverfolgung und biometrischen Identifizierung von Personen.
- Automatisierte Datenanalyse zur (auch „selbstlernenden“) Zusammenführung und Auswertung von Informationen auf einer KI-Plattform.
- Nachträgliche biometrische Identifizierung von Personen durch einen (weltweiten) Fotovergleich mit Internet-Daten.
- Das Entwickeln, Trainieren und Testen von KI-Modellen mit echten Polizeidaten.

Die KI bei der Polizei – 15: Wie genau sollen die neuen Polizei-KI-Systeme funktionieren?

Das weiß niemand so genau, auch nicht die Polizei, sie erhält eine „Black Box“. Denn zum einen existieren die Systeme, die mit dem Gesetzentwurf umschrieben werden, in dieser Form überwiegend noch gar nicht. Die Befugnisse sind gewissermaßen ein „Experiment“, allerdings eines mit den Daten vieler, in aller Regel unbescholtener Menschen. Zum anderen ist der Gesetzentwurf an entscheidenden Stellen vage und verlagert die Klärung von Detailfragen in untergesetzliche Vorschriften, die irgendwann später kommen sollen, ohne Einbindung des Parlaments. Diesen Ansatz halten wir für unzulässig: Bei speziellen Datenverarbeitungs-Befugnissen verlangt das Bundesverfassungsgericht ausdrücklich, dass alles Wesentliche, auch zum technischen Verfahren, im Gesetz selbst geregelt sein muss.

Die KI bei der Polizei – 16: Was verbirgt sich hinter der KI-Videoüberwachung?

Geplant ist ein mehrstufiges Verfahren. Demnach soll an bestehende Videoüberwachungen im öffentlichen Raum eine KI-Mustererkennung angeschlossen werden, um automatisch „verdächtiges Verhalten“ oder gefährliche Gegenstände zu erkennen und Alarm auszulösen. Gibt es einen Treffer, können Personen zur Nachverfolgung markiert, über weitere Videoübertragungen hinweg verfolgt und anhand biometrischer Fahndungsdaten aus der Ferne identifiziert werden. Hier sehen wir mehrere erhebliche Probleme.

Vorausgesetzt wird ein zuverlässiges Mustererkennungs-System, aber das gibt es nicht. Selbst mittels hochentwickelter Anwendungen dürfte es kaum möglich sein, eine Umarmung von einer Rangelei oder einen Besenstil von einem Knüppel zu unterscheiden. Die absehbare Folge ist eine Unmenge falsch-positiver Treffer, also wohl fast immer: Fehlalarme. Das ist besonders deswegen zu befürchten, weil öffentliche Videoüberwachungen in der Regel an sehr belebten Orten stattfinden.

Zudem muss man fragen, was genau mit diesem System eigentlich überwacht wird. Untechnisch gesehen handelt es sich um eine Art Bevölkerungs-„Verhaltensscanner“, dem alle Menschen ausgesetzt sind, die sich zufällig im Sichtbereich der

Videoüberwachung befinden. Das sind allerdings fast immer Menschen, die unbeteiligt und unbescholten sind. Selbst wenn sie es im Einzelnen nicht merken, weil die KI im Hintergrund arbeitet, werden ihre Daten erfasst und verarbeitet. Das ist ein massenhafter Grundrechtseingriff.

Wenn sich wirklich jemand gefährlich verhält, ist es die Aufgabe der Polizei, vor Ort zu sein und einzuschreiten. Die Identifizierung aus der Ferne trägt überhaupt nichts dazu bei, Gefahrensituationen professionell zu klären und Angriffe schnellstmöglich zu unterbinden.

Die KI bei der Polizei – 17. Was bedeutet automatisierte Datenanalyse?

Der Polizei soll es gestattet werden, Informationen aus so gut wie allen erdenklichen Datenbeständen zusammenzuführen, um Erkenntnisse zu gewinnen. Dafür soll eine KI-Plattform eingesetzt werden, bei Bedarf auch ein selbstlernendes System. Die Umschreibung im Gesetzentwurf weckt sofort Assoziationen mit Anbietern wie Palantir, und ungefähr daran dürften die Autoren des Innenministeriums auch gedacht haben. Genau solche umstrittenen Tools würden nicht nur für wenige Spezialfälle eingesetzt werden können, sondern stünden der alltäglichen Sachbearbeitung zur Verfügung. Auch hier sehen wir mehrere erhebliche Probleme.

Die automatisierte Datenanalyse ist natürlich effektiver als die händische Auswertung von Informationen. Sie leistet aber nicht nur viel mehr, sondern auch etwas ganz Anderes, als nur Daten in Excel-Tabellen schneller als manuell möglich zu sortieren und zu vergleichen, um relevante Treffer zu filtern. Sondern durch die sogenannte Datenfusion werden auch neue Erkenntnisse generiert und womöglich Verdachtsmomente erzeugt, die es ohne KI gar nicht gäbe.

In die KI-Datenanalyse einbezogen werden können nicht nur fallspezifische Daten, sondern so gut wie alle Informationen, die bei der Polizei gespeichert sind, etwa auch zu Zeuginnen und Zeugen, zu Hinweisgebenden und Geschädigten, zu vielleicht einfach nur rein zufällig einmal notierten Personen. Ihre Daten können in der KI-Plattform immer wieder mitverarbeitet werden. Dazu gehören auch Daten aus abgeschlossenen Vorgängen, die aus Polizeisicht längst nicht mehr relevant sind. Und: Auch wenn die KI-Plattform nicht direkt an das Internet angeschlossen sein soll, darf die Polizei Datensätze aus dem Internetdaten „nachschieben“. Die Datenanalyse hat damit gar keine erkennbaren Grenzen mehr.

Der Gesetzentwurf setzt voraus, dass die Verarbeitungsschritte bei der KI-Datenanalyse dokumentierbar sind, dass keine diskriminierenden Algorithmen angewandt oder ausgeprägt werden und alle Analyse-Ergebnisse hinterher nachvollziehbar bleiben. All das sind Voraussetzungen, die insbesondere auf selbstlernende Systeme gar nicht zutreffen, ganz zu schweigen davon, dass die gängigen KI-Modelle bekanntlich zum „Halluzinieren“ neigen.

Die KI bei der Polizei – 18: Was hat es mit der biometrischen Internet-Identifizierung auf sich?

Dieser Fall wird niemandem entgangen sein: Vor einer Weile gelang es Journalistinnen und Journalisten, das mutmaßliche frühere RAF-Mitglied Daniela Klette aufzuspüren. Dafür wurde ein KI-Tool genutzt, das anhand eines jahrzehntealten Fahndungsfotos im Internet eine aktuelle Aufnahme fand. Daraus ergaben sich nicht nur Hinweise auf Klettes heutiges Aussehen, sondern auch auf ihren Aufenthaltsort. Die sächsische Polizei will das jetzt auch tun dürfen: Fotos etwa von flüchtigen, vermissten oder noch unbekannt Personen biometrisch verarbeiten und dann das Internet nach ähnlichen Personen durchforsten. Hier sehen wir mehrere erhebliche Probleme.

Keine Frage, der neue „Klette-Paragraf“ wäre für die Polizei ein sehr nützliches Instrument. Aber die Anwendung verstößt aus Sicht der Fraktion Die Linke gegen europäisches Recht, konkret die sogenannte KI-Verordnung. Sie verbietet ausdrücklich KI-Systeme, mit denen ein biometrisch aufbereiteter Internet-Bildkatalog durchgerastert wird, um Gesichter zu erkennen.

Es gibt einige kommerzielle Anbieter, die genau diese Art der biometrischen Rasterfahndung für „Jedermann“ anbieten, und bei der Suche nach Klette kam wohl auch ein solcher Dienst zum Einsatz. Aber rechtmäßig ist das deshalb nicht, und wohl nicht zufällig haben bekannte Anbieter ihren Sitz außerhalb der EU. Der Gesetzentwurf löst dieses Problem nicht. Die sächsische Polizei erhält also eine Befugnis, die entweder technisch nicht umzusetzen oder aber anzuwenden verboten wäre. Das ist ein Unding für ein Polizeigesetz, das auf dem Boden der Grund- und Freiheitsrechte stehen muss.

Aber selbst, wenn es nicht verboten wäre oder wenn die sächsische Polizei überraschenderweise eine neue Methode für eine erlaubte Umsetzung fände: Die biometrische Internet-Identifizierung ist ein in dieser Art völlig neues globales Massenüberwachungs-Instrument. Jeder Mensch, egal woher, müsste es sich künftig gefallen lassen, dass die eigenen Abbildungen im Internet ausgelesen und durch eine sächsische Polizei-KI verarbeitet werden. Es liegt auf der Hand, dass dem heimlichen Vergleich so gut wie ausschließlich (und womöglich immer wieder) solche Personen unterzogen werden, die völlig unbescholten und unbeteiligt sind.

Die KI bei der Polizei – 19: Worauf zielt ein Polizei-eigenes KI-Modell?

Die vierte und letzte große KI-Befugnis im Gesetzentwurf soll es ermöglichen, dass die sächsische Polizei eigene KI-Modelle, egal ob regelbasiert oder selbstlernend, entwickeln, testen und anwenden kann. Der Clou ist: Wenn die Polizei das nicht selbst kann, womit zu rechnen ist, dann darf sie externe Anbieter damit beauftragen. Die Polizei darf dazu ihre „echten“ Datenbestände einspeisen. Und wenn die sich nicht komplett anonymisieren lassen, womit ebenfalls zu rechnen ist, dann können sogar Klartext-Daten an einen Auftragnehmer übermittelt werden. Hier sehen wir mehrere erhebliche Probleme.

Die Regelung lässt komplett offen, wozu die Befugnis eigentlich da ist. Klar: Alle vorgenannten Befugnisse erfordern Systeme, die auf die sächsische Polizei zugeschnitten werden müssen. Aber dabei belässt man es nicht, denn im Gesetzentwurf

heißt es: KI-Modelle dürfen entwickelt werden „zur Aufgabenerfüllung“. Die Polizei hat aber sehr viele und sehr weit gesteckte Aufgaben. Diese Entgrenzung halten wir für problematisch.

Die KI-Modell-Befugnis ermöglicht es, dass die Polizei fast alle ihrer Daten, die Millionen von Menschen betreffen dürften und hochsensible, sicherheitsrelevante Erkenntnisse umfassen, im Klartext an Dritte aushändigen kann. Das zu tun wäre eine krasse Gefahr für die öffentliche Sicherheit. Aber der Gesetzentwurf geht noch einen Schritt weiter: Diesen Dritten, wer immer das ist, kann auch gestattet werden, das mit sächsischen Polizei-Daten gefütterte KI-Modell weiterzuverwenden, wozu auch immer.

Daten, die bei der Polizei gespeichert werden, dürfen prinzipiell nur für bestimmte Zwecke verwendet werden und unterliegen Speicherfristen, nach deren Ablauf sie in der Regel zu löschen sind. Diese essenziellen Bestimmungen werden mit der KI-Modell-Befugnis pauschal unterlaufen.

Immerhin, der Gesetzentwurf enthält eine kleine Sicherheitsvorkehrung: Es ist untersagt, die zum Entwickeln und Trainieren verwendeten Polizeidaten wiederherzustellen oder zu de-anonymisieren. Allerdings ist unklar, wie genau das technisch sichergestellt werden soll. Es ist unklar, ob es überhaupt möglich wäre, einen Verstoß gegen dieses Verbot zu bemerken. Und selbst wenn, der Gesetzentwurf sieht dafür nicht einmal eine Strafe vor.

Die KI bei der Polizei – 20: Hat das alles irgendwas mit Palantir zu tun?

Wir befürchten das. Offiziell haben die Koalitionsfraktionen CDU und SPD vereinbart, auf den Einsatz von Palantir-Produkten zu verzichten. Allerdings handelt es sich um eine rein politische Verabredung. Sie ist ziemlich vage formuliert, betrifft nicht alle KI-Befugnisse und bleibt eine jederzeit veränderbare „Auslegungssache“. Der Gesetzentwurf selbst schließt mit keiner Silbe aus, dass später auf Palantir zurückgegriffen wird, und wer dem Gesetzentwurf zustimmt, nimmt das in Kauf. Wir halten es für sehr wahrscheinlich, dass die sächsische Polizei über kurz oder lang mit Palantir arbeiten wird. Denn aus Kostengründen und zum erleichterten Datenaustausch mit anderen Bundesländern wird man keine sächsische „Inselsysteme“ schaffen wollen, sondern auf eine bundeseinheitliche Lösung setzen. Dort stehen die Zeichen ebenfalls klar auf Palantir.

Die Vorstellung, dass höchstensible und sicherheitsrelevante Polizeidaten künftig massenhaft durch unkontrollierbare IT-Systeme ultrarechter Oligarchen verarbeitet werden, ist für die Fraktion Die Linke nicht annehmbar – und daher auch kein Gesetz, das das nicht definitiv ausschließt. Der Gesetzentwurf widerspricht durch seine erklärte „Anbieterneutralität“ zudem allen Bekundungen zur sogenannten digitalen Souveränität, mit der gewährleistet werden soll, dass rechtsstaatlich erhobene Daten den Raum europäischer Rechtsstaaten nicht verlassen, statt sich auf gefährliche Abhängigkeiten einzulassen. Klar ist allerdings auch: Die geplanten KI-Befugnisse genügen diesen Ansprüchen auch ohne Palantir nicht.