

Dr. Roland Wagner

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 C

Dr. Roland Wagner c/o Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, D-65185 Wiesbaden

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Antrag der CDU/CSU-Bundestagsfraktion: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ (20/9495), Anhörung des Ausschusses für Inneres und Heimat am 22. April 2024

Wiesbaden, 17. April 2024

Sehr geehrte Damen und Herren Abgeordnete,

für die Einladung, zum Antrag 20/9495 „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ vor dem Ausschuss für Inneres und Heimat des Deutschen Bundestages Stellung zu nehmen, darf ich mich sehr bedanken.

In dienstlicher Funktion bin ich als Landespolizeivizepräsident zuständig für die Sicherheit und den Schutz der etwas mehr als sechs Millionen hessischen Bürgerinnen und Bürger. Um dies zu gewährleisten, verrichten gut 20.000 Mitarbeiterinnen und Mitarbeiter tagtäglich Ihren zunehmend komplexer werdenden Dienst. Hierbei muss die Polizei vor allem in Zeiten der Digitalisierung und Globalisierung in der Lage sein, die exponentiell steigenden Datenmengen schnell und gezielt analysieren zu können, um regionale und überregionale Tat- und Täterzusammenhänge zu erkennen. Denn

es zeigt sich leider vermehrt: Es sind die kleinen Details, die oft den Unterschied zwischen einer verhinderten und einer vollendeten Tat ausmachen.

Zum Antrag der CDU/CSU-Bundestagsfraktion: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ – nehme ich wie folgt Stellung:

Vorbemerkung/Grundsätzliches

Einen ersten Grundpfeiler der Historie zum Thema polizeilicher Analysekompetenz stellt die Innenministerkonferenz im Jahr 2016 dar. Im Zuge dieser Innenministerkonferenz haben am 30. November 2016 die Innenminister der Länder sowie der damalige Bundesinnenminister die Saarbrücker Agenda unterzeichnet. Sie beschreibt die Neuausrichtung der Informationsarchitektur der Polizeien des Bundes und der Länder. Wesentliche Leitlinien waren dabei:

1. Jede Polizistin und jeder Polizist hat nach Maßgabe der rechtlichen Rahmenbedingungen jederzeit und überall Zugriff auf diejenigen Informationen, welche für ihre/seine Aufgabenerfüllung erforderlich sind.
2. Die zukünftige IT der Polizei ist einfach und anwenderfreundlich. Sie wird kontinuierlich dem jeweiligen Stand der Technik und den Anforderungen der IT-Sicherheit angepasst.
3. Polizeiliche IT-Angebote, die Bund und Länder gleichermaßen betreffen können, werden nur einmal entwickelt und stehen den Bedarfsträgern in den Ländern und im Bund zur Verfügung. Dadurch können Anforderungen aufgrund aktueller Entwicklungen zeitnah, flexibel und zuverlässig umgesetzt werden.
4. Die Grundlage für eine digitale, medienbruchfreie Vernetzung der Polizei mit ihren nationalen und internationalen Partnern wird geschaffen.

Anlass war die sich weltweit immer schneller ändernde Sicherheitslage. Denn die zunehmende digitale Vernetzung und Transformation unserer Gesellschaft stellten uns bereits damals vor neue sicherheitspolitische Herausforderungen. Die Geschwindigkeit der Veränderung hat sich seitdem noch einmal deutlich erhöht.

Die vernetzte Welt ermöglicht Kriminalität in einer neuen Dimension, über Grenzen hinweg und jederzeit. Man erkannte bereits damals die defizitäre Informationsarchitektur der Polizei und verständigte sich ausdrücklich auf eine

zukünftige IT der Polizei, welche kontinuierlich an den Stand der Technik, die Anforderungen der IT-Sicherheit sowie den Datenschutz angepasst wird, um die Polizistinnen und Polizisten in die Lage zu versetzen, auf diejenigen Informationen zugreifen zu können, die sie für ihre Aufgabenerfüllung dringend benötigen.

Nur kurze Zeit später, am 19. Dezember 2016, steuerte ein islamistischer Terrorist einen Sattelzug in eine Menschenmenge auf dem Berliner Breitscheidplatz. Er tötete 13 Menschen und verletzte weitere 67. Sie alle waren und sind Bürgerinnen und Bürger, die zuvor auf dem Weihnachtsmarkt zusammen mit Freunden und Familien die vorweihnachtliche Zeit genossen haben. Anis Amri war den Sicherheitsbehörden bekannt. Es gab mehrere Informationen aus unterschiedlichen Datenquellen, aber niemand konnte die Zusammenhänge erkennen.

Dieser und viele nachfolgende Anschläge wie in Halle auf eine Synagoge, beim Rosenmontagsumzug in Volkmarsen, der Terrorakt in Hanau oder die Umsturzpläne der Reichsbürgerszene, um nur einige traurige Beispiele zu nennen, stellen die Sicherheitsbehörden seitdem vor große Herausforderungen – mit deutlichem Einfluss auf das Sicherheitsgefühl der Bevölkerung.

Einher gehen der starke und wiederum schnelle gesellschaftliche Wandel, auch aufgrund steigender Radikalisierungsbereitschaft. Durch den Ukraine-Krieg und vor allem durch den Nahost-Konflikt hat sich die Sicherheitslage jüngst weiter verschärft. Die Wahrscheinlichkeit von Terroranschlägen hat sich nochmals deutlich erhöht.

Zentrales Ziel / Rechtsstaatlicher Auftrag

Dies alles verdeutlicht aus polizeilicher Sicht: Die Gefahr besteht nicht nur in ferner Zukunft, sie besteht nicht nur abstrakt. Sie kann sich vielmehr jederzeit konkretisieren. Angesichts dessen wird deutlich, wie wichtig es ist, unsere Innere Sicherheit zu stärken, um unsere Bevölkerung vor schwerwiegenden Gefahren zu schützen. Unser wesentliches Ziel, der Kern der Aufgaben unserer Sicherheitsbehörden ist es, Straftaten und Anschläge nicht nur zu verfolgen und aufzuklären, sondern möglichst vor der Tat einzuschreiten; wir wollen Gefahren abwehren, wir wollen die Menschen schützen bevor sich ein Anschlag oder eine andere Gefahrenlage realisiert.

Zentrale Frage: Einzeltäter vs. Täternetzwerk

Dabei hat sich spätestens seit dem Anschlag in den USA am 11. September 2001 und durch die schrecklichen Taten des NSU in Deutschland eine Frage – und vor allem die schnelle und zielsichere Antwort darauf – als wesentlich für den Erfolg oder Misserfolg unserer Bemühungen herausgestellt: Haben es die Sicherheitsbehörden mit Einzeltätern oder mit Täternetzwerken zu tun?

Dies zu erkennen und aus der Erkenntnis schnell und zielgerichtet die richtigen Maßnahmen abzuleiten, macht den entscheidenden Unterschied bei der Gefahrenabwehr aus. Insbesondere bei der Bekämpfung des Terrorismus, des Extremismus, aber auch bei der Bekämpfung der Schwere und der Organisierten Kriminalität wird die schnelle und umfassende Analyse eines Tatgeschehens zur zentralen Bedingung erfolgreicher Polizeiarbeit. Gerade hier sind unsere höchsten Rechtsgüter durch skrupelloses, oftmals menschenverachtendes Vorgehen in erheblichem Maße gefährdet. Dabei ist Zeit der entscheidende Faktor.

Dem Faktor der beschränkten Zeit stehen in der Regel gigantische Datenmengen gegenüber, die ausgewertet und miteinander in Verbindung gebracht werden müssen, um die handelnden Personen zu identifizieren, sie von der Tatausführung abzubringen und so Gefahren für die Bürgerinnen und Bürger abzuwehren.

Eine händische Auswertung der entstehenden Datenmengen ist längst nicht mehr möglich: Im Bereich der Bekämpfung des Missbrauchs von Kindern umfasst ein Vorgang im Durchschnitt ein Datenvolumen von 3,2 TB.

Ein Vorgang mit 3,2 TB entspricht etwas mehr als 5160 CD-Roms oder circa 745 DVDs. Den – natürlich rein rechnerischen – Vergleich mit Papierakten können wir indes bereits nicht mehr vornehmen. Mediendateien wie Bilder, Videos, Grafiken, Tonaufnahmen und dergleichen liegen darüber hinaus in unzähligen Formaten vor. Hinzu kommen spezifische Datenformate, die mit der hochfrequenten Nutzung von Smartphones, Tablets, Laptops und dergleichen einhergehen.

In einer einzelnen Datei in diesen Mengen könnte der Hinweis auf einen aktuellen Gefahrenüberhang und damit auf einen laufenden Missbrauch eines Kindes enthalten sein. Wenn wir den oben formulierten Anspruch der Gefahrenabwehrbehörden ernst nehmen, zeigt dies die dringende Notwendigkeit der schnellen und umfassenden

Datenanalyse, der – und das möchte ich an dieser Stelle betonen – ohnehin vorhandenen polizeilichen Datenbestände. Denn es geht bei der in Rede stehenden Analysefähigkeit nicht um Datengewinnung, sondern in erster Linie um die Auswertung bereits vorliegender Daten.

Das Grundproblem aller Sicherheitsbehörden ist jedoch, dass diese polizeilichen Datenbestände in einzelnen polizeilichen Datentöpfen separiert gespeichert sind. Es handelt sich um einzelne, teils historisch gewachsene, nicht originär verknüpfte Datensilos. Jedes dieser Silos muss manuell einzeln betrachtet werden, um dann zu versuchen, die gewonnenen Informationen miteinander zu vergleichen. Die entscheidenden Erkenntnisse aus diesen Daten sind also nicht schnell verfügbar und auch von Menschen auf Grund der Menge und Komplexität nicht mehr verarbeitbar.

Es ist daher mehr denn je dringend geboten, unsere polizeilichen Analyse- und Auswertestellen, unsere Ermittlerinnen und Ermittler personell, organisatorisch und insbesondere technisch zu stärken. Anders ist der Umgang mit derartigen Datenmengen nicht mehr möglich.

In Hessen erfolgte 2017 die Einführung der Auswerte- und Analyseplattform hessenDATA, mit der wir unmittelbar auf die Anschläge in Berlin, in Würzburg und bei unseren europäischen Nachbarn reagiert haben. Wir begegnen damit aber auch unseren eigenen Defiziten, die wir in der Bekämpfung des Terrorismus in der Vergangenheit ausgemacht haben. Dies gilt allen voran für die Geschehnisse um den Nationalsozialistischen Untergrund: Grundlage polizeilicher Entscheidungen muss immer eine sorgfältige und umsichtige Beurteilung der Lage sein. Je schlechter die Informationslage, umso höher das Risiko fehlerhafter Entscheidungen.

Es ist meine tiefe Überzeugung, dass wir unsere Sicherheitsbehörden befähigen müssen, gute Entscheidungen zu treffen. Entscheidungen, die im Sinne der Sicherheit unserer Bürgerinnen und Bürger sind und welche die Handlungsfähigkeit unserer Polizistinnen und Polizisten sicherstellen. Liegen der Polizei nicht die relevanten Informationen vor oder – noch fataler – kann die Polizei mit den ihr zur Verfügung stehenden Daten nicht richtig umgehen, ist eben diese Handlungsfähigkeit maßgeblich eingeschränkt. Im schlimmsten Fall können dann Anschläge oder schwere Straftaten nicht rechtzeitig verhindert werden. Wie bereits dargelegt, ist es elementar wichtig, schnell zu erkennen, ob Täter allein agieren oder ob sie Teil einer organisierten

kriminellen Gruppierung sind, ob und welche Sympathisanten, Unterstützer oder Mittäter im Umfeld zu finden sind und welche Gefahren wiederum von ihnen ausgehen. Die Bestätigung einer Einzeltätertheorie oder deren Widerlegung ist dabei in den letzten Jahren zu einem der höchsten Ansprüche an die Polizei geworden. Zu erkennen, ob ein Anschlag bevorsteht, ob ein laufender Angriff tatsächlich beendet wurde oder ob es weitere Ziele gibt, kann letztlich von einer einzigen Information abhängen, die der Polizei zwar möglicherweise vorliegt, aber eben auch erkannt und interpretiert werden muss.

Die folgenden Beispiele verdeutlichen, welche Relevanz das Instrument hessenDATA für die Hessische Polizei entfaltet hat. Sie sind exemplarisch für die verschiedenen Dimensionen und Aspekte polizeilicher Gefahrenabwehr zu verstehen. Gemeinsam führen sie klar vor Augen, wie wichtig diese Möglichkeit der Datenanalyse ist.

Konkrete Fallbeispiele

1. Anschlagsverhinderung Eschwege

Im Rahmen der internationalen Zusammenarbeit wurde das Polizeipräsidium Nordhessen durch das BKA im November 2017 über die Vorbereitungen eines Anschlags informiert. Die Informationen stammten aus den Posts eines Facebook-Profiles eines 17-Jährigen aus Eschwege. Erste Ermittlungen in Social Media erhärteten den Tatverdacht: Der Eschweger beschäftigte sich seit 2017 mit dem IS und sympathisierte seitdem mit dessen Ideologie.

Die im Anschluss beschlagnahmten 25 Social Media Accounts wiesen einen umgerechneten Umfang von ca. 100.000 DIN A4-Seiten bzw. 150 Aktenordner auf. Fünf Ermittlerinnen und Ermittlern und zwei Dolmetschern gelang es mit Hilfe der Analyseplattform hessenDATA innerhalb von drei Tagen, die Informationen zu strukturieren und die relevanten Informationen zusammenzustellen: Die große Faszination für den sogenannten Islamischen Staat und für dessen menschenverachtende Ideologie sowie die Überzeugung, der Jihad sei ein geeignetes Mittel im Kampf gegen Anders- oder Nichtgläubige, spiegelten sich in den fast 250.000 Chatbeiträgen wider. Weitere Brisanz erfuhr der Fall durch Informationen über

Kontakte zu einem britischen Gefährder und erste Probezündungen von Sprengkörpern.

In einer sofort veranlassten Durchsuchungsmaßnahme konnten innerhalb kürzester Zeit ein zur Veröffentlichung bestimmtes Bekennervideo und Sprengstoff sichergestellt werden. In der Beschuldigtenvernehmung gestand der Jugendliche die Anschlagsabsichten. Durch einen Kontakt im Irak sollte demnach dem Jugendlichen eine Sprengstoffweste übergeben werden, die dann im direkten Anschluss an einer vorgegebenen Örtlichkeit gezündet werden sollte.

2. Länderübergreifende Ermittlungen zu einem pädokriminellen Netzwerk

Der Polizei in Nordrhein-Westfalen (NW) gelang es, ein Netzwerk aus Pädokriminellen aufzudecken, der sogenannte Bergisch-Gladbach-Komplex. Die Maßnahmen der Ermittlerinnen und Ermittler führten dabei auch auf die Spur eines hessischen Mittäters. Gegen ihn und einen Haupttäter aus NW konnte der Verdacht des gemeinschaftlichen sexuellen Missbrauchs eines Kindes begründet werden. Daraufhin wurde seitens der Hessischen Polizei eine besondere Aufbauorganisation ins Leben gerufen, um weitere fortwährende Realmissbräuche zu verhindern. Ein exakter Zeitpunkt konnte jedoch von dem Kind nicht benannt werden und die Täter schwiegen zu den Vorwürfen.

Im Verlauf der Ermittlungen entschlossen sich die Beamtinnen und Beamten in Hessen zu einer Analyse der Daten von insgesamt 61 Asservaten mit mehreren Millionen Datensätzen mithilfe der Analyseplattform hessenDATA. Ziel war die Verhinderung weiterer Missbrauchstaten. Die Analyse erbrachte zunächst folgendes Ergebnis:

Beide Täter hielten sich zur gleichen Zeit in einem gleichnamigen (Name: Spain) WLAN-Bereich auf. Mithilfe der Auswertung von Geodaten in den Metadaten der zur fraglichen Zeit aufgenommenen Bilder konnte der WLAN-Bereich auf der Insel Mallorca in Spanien lokalisiert werden. Weitere darauf basierende Ermittlungen (Emails, Hotelbuchungen) bestätigten den gemeinsamen Aufenthalt der beiden Haupttäter auf der spanischen Insel und den Missbrauch des Schutzbefohlenen.

Die Analyse der Daten führte zu weiteren Ermittlungserfolgen: Es konnte erstens der Nachweis mehrerer Missbrauchstaten zum Nachteil von Kindern, die von mehreren Tätern gemeinschaftlich begangen wurden, erbracht werden. Zweitens konnte der Verdacht wegen des sexuellen Missbrauchs von weiteren Kindern im Alter von zwei bis elf Jahren begründet werden. Darüber hinaus wurde drittens bekannt, dass einem Täter ca. drei Monate zuvor ein 4-jähriges männliches Pflegekind anvertraut wurde. Die Maßnahmen mündeten viertens in einem weiteren Fall des sexuellen Missbrauchs eines Kindes, bei dem zur Tatbegehung die gefährliche – auch als Vergewaltigungsdroge bekannte – Substanz GBL eingesetzt wurde. Ein fünfter Ermittlungszweig führte zur Rettung eines einjährigen Pflegekindes aus den Händen eines weiteren Sexualstraftäters, welches ihm zwei Wochen zuvor anvertraut wurde.

Ohne die Nutzung von hessenDATA hätte die entscheidende Information über den Aufenthalt zur gleichen Zeit innerhalb eines WLAN-Netzes beider Hauptbeschuldigten nicht in kürzester Zeit erlangt werden können. Ohne die Nutzung von hessenDATA wären die weiteren Ermittlungen nicht in der Weise und in der Zeit herangereift, dass in letzter Konsequenz Missbrauchshandlungen verhindert wurden. Die Kinder hätten nicht schnellstmöglich aus der Hand ihrer Peiniger befreit werden können.

Die Beispiele könnten problemlos um eine Vielzahl weiterer ergänzt werden. An ihnen wird der Nutzen und die Bedeutung der Analysefähigkeit deutlich. Fachlich sind sich hierin alle Länder- und die Bundesbehörden einig.

Datenschutzrechtliche Aspekte und IT-Sicherheit

Bereits im Jahr 2018 entwickelte das Land Hessen auf Anregung und mit Unterstützung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit den §25a HSOG als spezialgesetzliche Regelung für die Automatisierte Anwendung zur Datenanalyse.

Die Norm ermächtigt die Hessische Polizei, in begründeten Einzelfällen zur Abwehr konkreter Gefahren für hochrangige Rechtsgüter die bereits vorhandenen polizeilichen Daten automatisiert zu analysieren, die dringend zur ganzheitlichen Beurteilung der Lage benötigt werden. Damit hat Hessen ein rechtliches Fundament für den ermittlungs- und auswertungsunterstützenden Einsatz moderner Technologie

geschaffen. Das Bundesverfassungsgericht hat mit Urteil vom 16.02.2023 (Az.: 1 BvR 1547/19, 1 BvR 2634/20) auf Grundlage des § 25a HSOG für Rechtsklarheit gesorgt und festgestellt, dass der Einsatz einer automatisierten Datenanalyse oder -auswertung grundsätzlich zulässig ist. Der hessische Gesetzgeber hat die Vorgaben, die das Gericht hierfür gemacht hat, unmittelbar aufgenommen und mit einer Novelle umgesetzt.

Selbstredend sind höchste Standards in Sachen IT-Sicherheit und Datenschutz notwendig. Moderner Datenschutz vollzieht sich in der Nutzung der Plattform selbst, bei jedem Nutzer, an jedem Tag und bei jedem Einsatz.

Dies bestätigend, wurde im Jahr 2023 durch das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) eine umfangreiche Quellcode-Prüfung des bayerischen Systems durchgeführt. Diese ergab, dass bezüglich des Systems keine Schwachstellen identifiziert werden konnten, die einen unzulässigen Abfluss von Daten unter Umgehung von Zugriffsbeschränkungen oder einen unautorisierten Zugriff von außen ermöglichen.

Europaweites Vergabeverfahren

Bund und Länder hatten sich zudem auf eine gemeinsame Beschaffung verständigt. Bereits im Jahr 2020 wurde durch den Verwaltungsrat des Polizei-IT-Fonds beschlossen, dass Bayern eine Öffnungs- und Nachnutzungsklausel in die Ausschreibung des Projekts „VeRA“ aufnimmt. Nach Bedarfsabfrage wurde Anfang des Jahres 2021 die Ausschreibung europaweit veröffentlicht und im März 2022 der Zuschlag an eine Firma erteilt. Im Ergebnis konnte nur ein Anbieter den Anforderungen gerecht werden.

Fazit

Moderne Kriminalitätsbekämpfung und höchste Ansprüche an den Datenschutz setzen den Einsatz moderner Technologie voraus, um den bestmöglichen Schutz der Bevölkerung zu ermöglichen.

Unsere Polizei muss in die Lage versetzt werden, zur Abwehr von Gefahren für höchste Rechtsgüter die eigenen Datenbestände schnell und effizient zu sichten, um auf dieser Grundlage die richtigen polizeilichen Entscheidungen treffen zu können. Darauf haben die Menschen in Hessen und Deutschland einen Anspruch. Sie zu schützen ist unsere Pflicht.

Die Analyseplattform „VeRA“ sollte dabei ein wesentlicher Baustein der gemeinsamen Sicherheitsarchitektur der Länder und des Bundes unter dem Dach von P20 werden.

Eine wesentliche Leitlinie der Saarbrücker Agenda war und ist, jeder Polizistin und jedem Polizisten die Daten zur Verfügung zu stellen, die für die polizeiliche Aufgabenerfüllung benötigt werden. Dies wird in Hessen, Nordrhein-Westfalen und Bayern durch die Einführung einer Analyseplattform sichergestellt.

Die fachliche Lücke an Analysefähigkeiten in den Polizeien der Länder und des Bundes, die durch ein Fehlen eines solchen Analysewerkzeugs entsteht, ist groß und gefährdet ganz aktuell die Sicherheit der Bürgerinnen und Bürger.

Das Streben nach digitaler Souveränität ist wichtig, nach hiesiger Einschätzung perspektivisch alternativlos und Teil der Digitalstrategie der hessischen Polizei. Dies bedeutet jedoch ausdrücklich nicht, zwingend erforderliche Technologien nicht zu nutzen, wenn sie derzeit von deutschen Firmen nicht geliefert werden können. Ein gegenwärtiges Zuwarten auf eine mögliche Entwicklung entsprechender Analysefähigkeiten ist aufgrund der bestehenden Herausforderungen und der Gefährdungslage fachlich keine Alternative.

Im Ergebnis ist es aufgrund des dargestellten Mehrwertes vielmehr fachlich dringend notwendig, die Polizeien der Länder sowie des Bundes unmittelbar mit einer Analyseplattform zu befähigen und die Handlungsfähigkeit unserer Sicherheitsbehörden bestmöglich auszubauen.

