20. Wahlperiode

Drucksache **20/3266**

HESSISCHER LANDTAG

15. 02. 2021

Kleine Anfrage

Torsten Felstehausen (DIE LINKE) vom 21.07.2020

Datenbanken, personengebundene und ermittlungsbezogene Hinweise bei der Hessischen Polizei

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Minister des Innern und für Sport:
Die hessische Polizei sorgt für die Sicherheit aller Bürgerinnen und Bürger in unserem Land. Dies tut sie durch ihren täglichen Einsatz und mithilfe modernster Technik. Für eine effektive Verbrechensbekämpfung und Gefahrenabwehr ist es unabdingbar, dass unseren Polizistinnen und Polizisten relevante Informationen schnellstmöglich zur Verfügung stehen. Die polizeilichen Auskunftssysteme sind daher ein elementares Arbeitsmittel für die Polizei und unerlässlich für die Sicherheit der Bürgerinnen und Bürger.

Der hessischen Polizei stehen für den dienstlichen Gebrauch verschiedene eigene polizeiliche Datensysteme sowie sogenannte Verbunddateien im Austausch mit anderen Bundesländern sowie dem Bundeskriminalamt und dem europäischen Ausland zur Verfügung.

Der Gesamtdatenbestand des polizeilichen Informationssystems beträgt etwa 19 Mio. Datensätze aus dem Bereich der Personen- und Sachfahndung. Im Bereich der Personensuche beläuft sich die Zahl der Anfragen auf ca. 45.000 pro Tag. Diese Abfragen sind ausschließlich im dienstlichen Kontext zulässig.

Alle Abfragen in polizeilich zugänglichen Datensystemen werden protokolliert. Die Protokollierung erfolgt aufgrund datenschutzrechtlicher Anordnung sowie aufgrund der Vorgaben der IT-Sicherheit.

Die Beamten werden regelmäßig darüber belehrt, was durch die Behörde dokumentiert wird. Bei Verdacht von Missbrauchsfällen werden behördeninterne Ermittlungen eingeleitet, und bei Bedarf wird das Hessische Polizeipräsidium für Technik zur technischen Auswertung hinzugezogen.

Im Hinblick auf die noch effektivere Unterbindung unberechtigter Abfragen im polizeilichen Auskunftssystem wurden bereits seit 2018 eine Vielzahl verschiedener Maßnahmen in technischer, rechtlicher und organisatorischer Hinsicht initiiert und umgesetzt:

Es wurde eine Arbeitsgruppe eingesetzt, die sich mit der übergreifenden Betrachtung der im Zusammenhang stehenden Aspekte IT-Sicherheit und Datenschutz befasste.

Alle Polizeibeschäftigten wurden hinsichtlich der geltenden Rechts- und Vorschriftenlage und die Polizeibehörden hinsichtlich der vor Ort wahrzunehmenden Dienst- und Fachaufsicht sensibilisiert.

Es wurden technische Maßnahmen im polizeilichen Auskunftssystem sowie technische Maßnahmen infrastruktureller Art zur Optimierung der Rahmenbedingungen wie etwa Anhebungen der Netzbandbreite nicht mehr ausreichend angebundener Dienststellen geprüft und umgesetzt.

Vor dem Hintergrund der aktuellen Vorfälle ist es das oberste Ziel der hessischen Sicherheitsbehörden, Vertrauen zu schaffen und zurückzugewinnen. Bestehende Strukturen und Abläufe werden fortlaufend auf den Prüfstand gestellt, mit großer Intensität weiterentwickelt und seit Juli 2020 noch weitere Maßnahmen initiiert.

Eingegangen am 15. Februar 2021 · Bearbeitet am 15. Februar 2021 · Ausgegeben am 15. Februar 2021
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Zunächst wurden die Passwörter aller Polizistinnen und Polizisten und der Beschäftigten zurückgesetzt und mussten neu vergeben werden. Die Passwortsicherheit wurde weiterhin erhöht, indem künftig bereits alle 21 Tage ein Passwortwechsel erforderlich ist.

Es erfolgte eine Belehrung durch den direkten Vorgesetzten und die erneute schriftliche Verpflichtung zur absoluten Geheimhaltung der persönlichen Kennung.

Diese Maßnahmen sollen dazu dienen, eine Zugriffsmöglichkeit durch Dritte zu erschweren. Einzig ausgenommen von der Aktivierung der Bildschirmsperre sind Standardarbeitsplätze der Leitstellen, da ansonsten in diesen hochkritischen Bereichen (Notrufannahme, Bearbeitung Überfallmelder, Einsatzführung etc.) die polizeiliche Arbeitsfähigkeit derart beeinträchtigt wäre, dass eine polizeiliche Aufgabenerfüllung gefährdet wird.

Diese Standardarbeitsplätze haben grundsätzlich einen fest zugewiesenen Benutzer pro Dienstschicht und stehen in besonders zutrittsgeschützten Bereichen. Alle anderen getroffenen Maßnahmen und Sicherheitsvorschriften gelten auch für die Standardarbeitsplätze der Leitstellen uneingeschränkt.

Darüber hinaus aktiviert sich der Sperrbildschirm bereits nach drei statt bislang 15 Minuten. Die Felder „Veranlasser“ und „Abfragegrund“ sind bei Abfragen im polizeilichen Auskunftssystem POLAS systemseitig verpflichtend auszufüllen. So werden u.a. Abfragen auf Veranlassung Dritter besser dokumentiert.

Diese Verpflichtung wurde auch organisatorisch per Erlass auferlegt. Seit dem 16. September 2020 ist in Hessen die Befüllung der Felder technische Voraussetzung für die Absendung der Rechercheabfrage. Nach wie vor wird jede Abfrage im Hintergrund des Programms protokolliert, so dass bei Auftreten von Zweifeln an der Rechtmäßigkeit der Abfrage, diese auch nachträglich überprüft werden kann.

Zudem wurden die Intervalle der bereits verwendeten Zufallskontrolle für das polizeiliche Auskunftssystem POLAS von jeder 200. auf jede 50. Abfrage deutlich verkürzt. Dies erhöht den Druck, alle Felder sorgfältig auszufüllen. Das Zusammenspiel der Maßnahmen führt damit dazu, dass Verstöße zeitnah festgestellt werden können.

Zwischenzeitlich ist außerdem auf Rechnern im Wachbereich aller hessischen Polizeistationen und -reviere der sogenannte „schnelle Benutzerwechsel“ eingerichtet worden. Dieser ermöglicht es, dass sich Polizeibeamte oder Polizeibeamtinnen als zusätzliche Nutzer an einem Rechner anmelden können, der bereits durch eine andere Person genutzt wird. Somit entsteht kein Zeitverzug, der durch das Abmelden des vorherigen Nutzers bedingt wäre.

Zugleich wurde und wird die Anzahl der Rechner im Wachbereich der Reviere und Stationen erhöht, um paralleles Arbeiten mehrerer Polizistinnen und Polizisten an unterschiedlichen Rechnern an der Wache zu gewährleisten.

Am 31. Auguste 2020 wurde ferner die Auflösung des sog. SingleSignOn umgesetzt. Das bedeutet, dass der Aufruf der einzelnen polizeilichen Auskunftssysteme nur noch mit einem zusätzlichen Passwort möglich ist. Auch das trägt dazu bei, die eventuelle missbräuchliche Nutzung dieser Systeme zu minimieren.

Jetzt muss sich der Nutzer zunächst mit separater Kennung anmelden, um eine Abfrage durchführen zu können. Erst mit diesem Login („Session“) kann der Nutzer die Abfragesysteme nutzen. Damit verknüpft ist die Einführung einer Abmeldefunktion in den Auskunftssystemen.

Der in der Polizeistation Rüsselsheim laufende Pilotversuch zu der Nutzung biometrischer Zugänge zu Rechnern wurde mittlerweile erfolgreich abgeschlossen. Es handelt sich um Handvenenscanner, mit denen eine Anmeldung schnell und unkompliziert an den damit eingerichteten Rechnern möglich ist. Unter Würdigung und Beachtung technischer und datenschutz-/arbeitsschutzrechtlicher Aspekte wird aktuell geprüft, alle Wachen der hessischen Polizeireviere und -stationen damit auszustatten.

Ein Erörterungsgespräch mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit hat bereits stattgefunden. Die Verwendung von Handvenen als biometrisches Merkmal hat unter anderem die Vorteile einer besonders hohen Genauigkeit und Fälschungssicherheit.

Im Rahmen der Prüfung einer Verwendung von Mobiltelefonen als zusätzliche Authentifizierungsmöglichkeit mittels Token Code werden auch weitere biometrische Merkmale (Gesichtserkennung und Fingerabdruck) getestet.

Darüber hinaus befinden sich die folgenden weiteren Maßnahmen in Prüfung:
Hierzu gehört die Nutzung biometrischer Merkmale auch für den Zugang zu den Auskunftssystemen ebenso wie die Nutzung technischer oder biometrischer Funktionen dienstlicher Smartphones, um sich darüber an Standardarbeitsplätzen und Auskunftssystemen zu authentifizieren.
Zudem werden technische und rechtliche Möglichkeiten zur Erstellung bzw. Erweiterung einer Abgleichliste von „Personen des öffentlichen Lebens“, deren Abfrage eine zusätzliche Bestätigung erforderlich macht, geprüft.

Des Weiteren erhalten die Datenschutzbeauftragten der Polizeibehörden zusätzliche Ressourcen und wo nötig Personal, um ihrer wichtigen Aufgabe nachzukommen.

Zusätzlich zu den bereits dargestellten Maßnahmen in technischer, rechtlicher und organisatorischer Hinsicht erfolgt eine gesamtorganisatorische Betrachtung bezüglich der Thematik Datenschutz im neu aufgesetzten Projekt „Sichere Daten“. Dabei sollen unter anderem bestehende Prozesse überprüft werden, um so Regelungsbedarfe zu identifizieren. In diesem Zusammenhang werden auch die Benutzer- und Rollenkonzepte evaluiert und in Abhängigkeit dessen, bedarfsorientiert angepasst.

Die Vorbemerkung vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1. Auf welche Datenbanken hat die hessische Polizei zur Erfüllung ihrer Aufgaben im Bereich Strafverfolgung, der Gefahrenabwehr und der allgemeinen Verwaltung Zugriff? Bitte eine detaillierte Einzelauflistung nach Datenbanken und Systemen.

Die hessische Polizei hat zur Erfüllung ihrer Aufgaben im Bereich der Strafverfolgung, der Gefahrenabwehr, aber auch der allgemeinen Verwaltung im Rahmen der jeweils geltenden Berechtigungen Zugriff auf folgende Datenbanken:

Bezeichnung

- Elektronische Bildbearbeitung (EBV),
- Elektronisches Tätigkeitsbuch (ETB),
- Elektronische Unfalltypensteckkarte (Euska),
- Kriminalitätslagebild - neu (KLB),
- KLB-Operativ,
- Crime,
- Sonderlagen (SOLA),
- einheitliches Fallbearbeitungssystem (eFBS),
- Polizeilicher Informations- und Analyseverbund (PIAV) Operativ-Zentral,
- INPOL-FALL,
- Polizeiliches Auskunftssystem (POLAS) [LAND / INPOL / Schengen (SIS)],
- DNA Analyse Datei (DAD),
- AFIS-Sofortauskunft,
- Polizeiliche Kriminalstatistik (PKS),
- Computergestützte Vorgangsbearbeitung (ComVor),
- ComVor-Index (CV-I),
- Discoverer/SplashBI,
- Einwohnermeldeauskunft (EWO Meldedatenabfrage),
- EWO-Fahndungsabgleich,
- Lichtbildrecherche,
- Tatortberechtigten-Datenbank,
- Nationales Waffenregister (NWR),
- Ausländerzentralregister (AZR) mit den Modulen VISA, VIS, VIS-FastID,
- Justiz Online mit den Modulen ZStV, BZR, ECRIS,
- Kraftfahrt-Bundesamt mit den Modulen ZFER, ZFZR, FAER FE, FAER online, EUCARIS, ZKR, TACHONET (KBA/“ZEVIS“),
- Fahrzeugteileauskunft (FADA),
- Schiffskontrolldatei (SKD),
- Rechtsextremistendatei (RED),
- Antiterrordatei (ATD),
- Owi21,
- Owi21 ToGo,

- Einsatzführungssystem (EFS), (Leitstellenmodul AAO, Befehlsstellenmodul BAO),
- HessenData,
- Zuverlässigkeits- und Sicherheitsprüfung (SÜP),
- Darex (Datenbank Rechtsextremismus (Tonträger)).

Frage 2. Haben die berechtigten Dienstkräfte der Hessische Polizei Zugriff auf Datenbanken anderer Bundesländer und/oder des Bundes?
Wenn ja, auf welche und aufgrund welcher Rechtsgrundlage jeweils? Bitte eine detaillierte Einzelauflistung nach Datenbank und Systemen.

Berechtigte der hessischen Polizei haben zur Wahrnehmung Ihrer Aufgaben Zugriff auf folgende IT-Verfahren anderer Bundesländer und des Bundes:

Ebene	Abkürzung	Anmerkung	Rechtsgrundlage
Bund	ABS	Abgleichservice Oberflächenloses System, wird nur über den AFM im Zusammenhang mit SÜP genutzt.	§ 29 BKAG
Bund	AFIS	Daktyloskopische Datenbank	§ 29 BKAG
Bund	BZR	Bundeszentralregister	§ 41 BZRG
Bund	PIAV	PIAV-O-Z: Waffen- und Sprengstoffkriminalität; Rauschgiftkriminalität; Cybercrime; Eigentumskriminalität und Vermögensdelikte; Dokumentenkriminalität; Schleusung; Menschenhandel; Ausbeutung	§ 29 BKAG
Bund	INPOL-Fall	APOK; Falschgeld; Geldwäsche; IFIS; Korruption; VUTOT; Wikri	§ 29 BKAG
Bund	INPOL-Z	Personen-, Sach- und Falldaten	§ 29 BKAG
Bund	RED	Rechtsextremistendatei	§ 29 BKAG
Bund	ATD	Antiterrordatei	§ 1 ATDG
Bund	DAD	DNA Analyse Datei	§ 29 BKAG
Bund	AZR	Ausländerzentralregister	§ 15 AZRG
Bund	NWR	Nationales Waffenregister	§ 10 NWRG
Bund	KBA	Kraftfahrt-Bundesamt mit den Modulen ZFER, ZFZR, FAER FE, FAER online, EUCARIS, ZKR, TACHONET (KBA/“ZEVIS“)	§ 36 i.V.m §35 StVG
Bund/ KFZ-Hersteller	FADA	Fahrzeugteileauskunft	
Alle Bundesländer		Melderegister	§ 38 i.V.m. § 34 BMG

Frage 3. Haben der Bund und/oder die Länder Zugriff auf die Datenbanken der hessischen Polizei oder anderer hessischer Behörden?
Wenn ja, auf welche Datenbanken, auf welcher Rechtsgrundlage, durch wen und wie ist der jeweilige Datenzugriff bzw. die Datenübermittlung ausgestaltet?

Der Bund und/oder die Länder haben keinen Zugriff auf die Datenbanken der hessischen Polizei.

Die Behörden des Bundes und der Länder haben Zugriff auf die Melderegister.

Grundsätzlich gilt: Anderen öffentlichen Stellen im Sinne von § 2 Abs. 1 bis 3 und 4 Satz 2 des BundesdatenschutzG darf die Meldebehörde die Daten aus dem Melderegister übermitteln, soweit dies zur Erfüllung der in ihrer Zuständigkeit liegenden öffentlichen Aufgaben erforderlich ist (§ 34 Bundesmeldegesetz (BMG)).

Das BMG ermöglicht den automatisierten Abruf der in § 38 BMG genannten Daten. Entsprechend der Ermächtigung des § 55 BMG wurde der Umfang der übermittel- bzw. abrufbaren Daten für bestimmte Behörden in der Hessischen Meldedatenübermittlungsverordnung (HessMeldDÜV) erweitert. Für die in § 34 Abs. 4 genannten Sicherheitsbehörden besteht in Hessen ein sogenannter Datenpool, d.h. ein Spiegel aller hessischen Melderegister, der eine hessenweite Abfrage der für die Arbeit der Sicherheitsbehörden erforderlichen Daten ermöglicht, während die sonstigen Behörden in Hessen Daten jeweils nur bei einer bestimmten Meldebehörde abfragen können. § 39 Abs. 1 BMG verpflichtet die abrufberechtigte Stelle durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass Daten nur von hierzu befugten Personen abgerufen werden können.

Ist im Melderegister eine Auskunftssperre nach § 51 BMG eingetragen, erhält die abrufende Stelle eine Mitteilung, die keine Rückschlüsse darauf zulassen darf, ob zu der betroffenen Person keine Daten vorhanden sind oder eine Auskunftssperre besteht. In diesen Fällen ist der Abruf von der Meldebehörde wie ein Ersuchen um Datenübermittlung nach § 34 zu behandeln, d.h. die Anfrage wird dann manuell weiterbearbeitet.

Die Standards der Datenübermittlung ergeben sich aus § 3 der Ersten Bundesmeldedatenübermittlungsverordnung vom 1. Dezember 2014 (BGBl. I S. 1945), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2745). Sie gelten entsprechend auch im Hinblick auf die Datenübermittlungen gem. HessMeldDÜV.

Frage 4. Sind dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit das Berechtigungskonzept der Datenbanken und die jeweiligen Zugriffsrechte bekannt?
a) Wenn nein, warum nicht?
b) Inwiefern wird der Hessische Beauftragte für Datenschutz und Informationsfreiheit in die oben genannten Prozesse (Erteilung neuer Zugriffsbefugnisse etc.) mit einbezogen bzw. darüber informiert?

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) ist vor der Inbetriebnahme von neu anzulegenden Dateisystemen zu konsultieren, wenn die Voraussetzungen des § 64 Abs. 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vorliegen. Dabei sind ihm die in § 64 Abs. 2 HDSIG genannten Unterlagen und Angaben vorzulegen. Insoweit Änderungen vorgenommen werden müssen, die unter die Vorgaben des § 64 HDSIG fallen, wird der ebenfalls HBDI informiert.

Zudem kann der HBDI sämtliche Berechtigungskonzepte der jeweiligen Datenbanken stets zur Erfüllung seiner Aufgaben seitens der hessischen Polizei anfordern (§ 14 Abs. 4 HDSIG). Etwaige Fragen betreffend die Zuständigkeit des HBDI, insbesondere ob sämtliche Berechtigungskonzepte der jeweiligen Datenbanken dem HBDI sind, können direkt an den HBDI als unabhängige oberste Landesbehörde gerichtet werden.

Frage 5. Welche verschiedenen personengebundenen und ermittlungsbezogenen Hinweise bzw. Werte (PHW/EHW) sind in den Datenbanken der hessischen Polizei gespeichert und standardisiert auswählbar? Bitte einzeln nach selektierbaren Hinweisen / Wertenauflisten.

Die Frage kann in Bezug auf die ermittlungsbezogenen Hinweise (EHW) nicht offen beantwortet werden, da sie detaillierte Einzelheiten zu ermittlungstaktischen Verfahrensweisen, aus deren Bekanntwerden Rückschlüsse auf Vorgehensweise, Fähigkeiten und Methoden der Ermittlungstätigkeit der Polizeibehörden gezogen werden könnten, enthält. Auf Grund dessen sind diese Informationen nicht zur Veröffentlichung geeignet.

Bei PHW können berechtigte Nutzer aus einem Katalog genau einen Wert auswählen. Das Hinterlegen mehrerer PHW ist möglich. Die aufgeführten Hinweise sind im System auswählbar:

Personengebundener Hinweis:

- Bewaffnet,
- gewalttätig,
- Ausbrecher,
- Ansteckungsgefahr,
- psychische- und Verhaltensstörungen,
- BTM-Konsument,
- Freitodgefahr,
- Halter/Führer gefährlicher Tiere,
- Explosionsgefahr,
- Häusliche Gewalt.

Frage 6. Wie viele Personen in der Hessischen Polizei haben eine Zugangsberechtigung zu den diversen polizeilichen Datenbanken? Bitte nach Datenbank auflisten.

In der hessischen Polizei werden Zugriffsberechtigungen je nach Zuständigkeit und Rolle anhand von Rechte- und Rollenkonzepten administriert und einzelnen Berechtigten bedarfsorientiert individuell zugewiesen. Eine Berechtigung erfolgt ausschließlich auf Antrag, der über mehrere Hierarchieebenen auf Rechtmäßigkeit geprüft wird. Bei einem Tätigkeits- oder Rollenwechsel werden Berechtigungen entfernt und müssen aufgabenorientiert neu beantragt werden. Die Anzahl der berechtigten Polizeibeschäftigten variiert stark nach Funktion und insbesondere auch im Hinblick auf die im jeweiligen System hinterlegten Daten. So hat beispielsweise aus Geheimschutzgründen eine Anzahl von Personen im sehr niedrigen einstelligen Bereich Zugriff auf die Antiterrordatei während jeweils rund 17.000 Beschäftigte Zugriff auf die Systeme „EWO“, „ZEVIS“ oder „POLAS“ haben. Darüber hinaus kann keine vollständige Auflistung aller Zugriffsberechtigungen erfolgen, da diese weitreichenden Rückschlüsse auf die Arbeitsweise und Leistungsfähigkeit der polizeilichen IT-Infrastruktur zulassen würden.

Frage 7. Welche PHW/EHW wurden wie oft in den Jahren seit 2010 jeweils neu angelegt? Bitte nach Jahr und PHW/EHW aufschlüsseln.

In Bezug auf die EHW-Hinweise wird auf die Beantwortung der Frage 5 verwiesen.

Da keine Statistiken geführt und LOG-Tabellen von POLAS nach zwei Jahren, von EWO nach einem Jahr und von ZEVIS nach sechs Monaten bereinigt werden, ist nur eine Aussage über den aktuellen Bestand möglich. Eine Auswertung erfolgte zum Stichtag 30. Juli 2020 und ist der Anlage zu entnehmen. Im Rahmen der Auswertung wurden personenbezogene Hinweise (PHW) berücksichtigt, welche in den letzten zehn Jahren gespeichert wurden. Löschungen innerhalb dieses Zeitraumes können nicht berücksichtigt werden, weil innerhalb des Systems darüber keine Dokumentation erfolgt.

Wiesbaden, 31. Dezember 2020

Peter Beuth

Anlagen

PHW	**Anzahl der Datengruppen gespeichert im Jahr**									
	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
BEWAFFNET	815	852	764	788	873	976	1.557	1.875	1.719	858
GEWALTTÄTIG	2.315	1.930	1.582	1.812	1.912	1.833	2.065	2.510	2.776	1.510
AUSBRECHER	2	1	3	0	1	1	1	0	0	0
ANSTECKUNGSGEFAHR	5	117	71	86	42	58	48	54	48	20
PSYCHISCHE UND VERHALTENSSTÖRUNGEN	78	70	74	50	69	103	165	173	182	151
BTM-KONSUMENT	4.271	4.078	3.993	4.727	5.037	5.570	7.000	8.565	8.506	3.807
FREITODGEFAHR	Fristablauf (FA)	FA	FA	FA	FA	FA	FA	41	103	36
HALTER/FÜHRER GEFÄHRLICHER TIERE	0	0	0	0	2	1	1	4	1	0
EXPLOSIVSTOFFGEFAHR	11	14	15	18	15	28	38	43	32	16
HÄUSLICHE GEWALT	2.757	2.719	2.695	2.621	2.855	3.031	3.687	4.527	4.172	2.537