

**Kleine Anfrage****Torsten Felstehausen (DIE LINKE) vom 20.05.2019****Hessendata – Teil 1****und****Antwort****Minister des Innern und für Sport****Vorbemerkung Fragesteller:**

Die von der hessischen Polizei genutzte Software Hessendata verknüpft für die automatische Datenanalyse umfangreiches Datenmaterial aus verschiedenen polizeilichen Datenbanken und sozialen Medien. Auch Daten anderer öffentlicher und nicht-öffentlicher Stellen können gemäß § 26 HSOG für den automatischen Datenabgleich hinzugezogen werden. Bei der Analyse geht es darum, Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen herzustellen und die eingehenden Erkenntnisse zu bekannten Sachverhalten zuzuordnen und gespeicherte Daten statistisch auszuwerten. Die Anwendung von Hessendata hat eine hohe Eingriffsintensität. Die automatisierte Datenanalyse ermöglicht durch die Kombination einer großen Menge an Daten aus unterschiedlichen Quellen umfassende Persönlichkeitsbilder und die Offenlegung sozialer Netzwerke und Strukturen. Durch die komplexen Verarbeitungs- und Verknüpfungsmöglichkeiten gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt.

Vorbemerkung Minister des Innern und für Sport:

Im Rahmen der Sicherheitsstrategie 2016 bis 2020 für die hessische Polizei hat die Hessische Landesregierung unter anderem auch den Staatsschutz mit einem umfassenden Maßnahmenpaket gestärkt. Dieses beinhaltet als ein Element die personelle, organisatorische und technische Stärkung der Analyse- und Auswertestellen. In diesem Zusammenhang wurde die Analyseplattform „hessenDATA“ implementiert und in die polizeiliche Ermittlungsarbeit integriert. Sie ermöglicht eine effektive und effiziente Gefahrenabwehr. Analysten, Ermittler und Operativkräfte der Polizeipräsidien und des Landeskriminalamts arbeiten gemeinsam an der Analyseplattform „hessenDATA“. Wichtigstes Ziel dabei ist, Terroristen und Schwerstkriminelle effektiv zu bekämpfen und Anschläge zu verhindern. Mit hessenDATA kann die Polizei bereits vorhandene Informationen aus polizeilichen Datenbanken schnell und richtig verknüpfen und damit schnell gebündelte Erkenntnisse – zum Beispiel über islamistische Gefährder – generieren. Die in den Datenbanken enthaltenen Daten wachsen rasant und sind heterogen in Qualität und Formaten. Eine schnelle und präzise analytische Zusammenführung („Datenmatching“) ist notwendig, um diese Bestände optimal zu erschließen. Dadurch können Gefahren rechtzeitig erkannt und Ermittlungen zu einschlägigen Straftaten zielgerichtet und erfolgreich geführt werden. Die Analyseplattform hilft Netzwerke aufzuhellen und kann dadurch Menschenleben retten. Informationsverarbeitung ist für die Sicherheitsbehörden im Zuge der Digitalisierung ein integraler Bestandteil des Schutzes der Bevölkerung geworden. Schnelles und frühzeitiges Erkennen bedrohlicher Strukturen ermöglicht im günstigsten Fall ein Einschreiten vor dem Schadenseintritt.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1. Wie viele Anordnungen gem. § 25a III HSOG für Hessendata gab es bisher?

Fünf generelle phänomenbezogene Anordnungen gemäß § 25a III HSOG, unter Einbindung des Hessischen Datenschutzbeauftragten, liegen bisher vor (Stand Juni 2019).

Frage 2. Bezieht sich eine Anordnung gem. § 25a III HSOG typischerweise auf eine Person oder auf mehrere?
Wenn Letzteres, auf wie viele im Durchschnitt?

§ 25a III HSOG sieht eine Einzelfallprüfung vor. Es handelt sich bei einem Einzelfall im Sinne des § 25a HSOG nicht um ein einzelnes Ermittlungsverfahren, sondern um einen Vorgang bzw.

ein Projekt, das an ein Ermittlungsverfahren anknüpft. Da ein solcher Vorgang bzw. Projekt eine oder mehrere Personen betreffen kann, kann keine allgemein gültige Aussage über die durchschnittliche Anzahl der betroffenen Personen getroffen werden.

Frage 3. Wird Hessendata nur präventiv-polizeilich genutzt oder auch zu strafprozessualen Zwecken? Ist bei der vorbeugenden Bekämpfung von Straftaten gem. § 25a I HSOG eine konkrete Gefahr erforderlich?

Die Daten in der Analyseplattform werden präventiv-polizeilich gespeichert und verarbeitet. Die Abfragen dienen zeitgleich präventiv-polizeilichen und strafprozessualen Zwecken (sog. doppel-funktionale Maßnahmen). Schwerpunktmäßig wird die Software „hessenDATA“ zur Abwehr von terroristischen Gefahren landesweit bei den Staatsschutzdienststellen eingesetzt, sowie zur Bekämpfung der Organisierten und Schweren Kriminalität, beispielsweise die Bekämpfung des Wohnungseinbruchsdiebstahls sowie Straftaten zum Nachteil älterer Mitbürger und Kapitaldelikte. Der Gefahrenbegriff gemäß § 25a I HSOG bezieht sich auf die Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

Frage 4. Aus welchen Quellsystemen wird Hessendata gespeist? Bitte gliedern nach Datenbanken/-beständen von Sicherheitsbehörden des Landes Hessen (z.B. POLAS, ComVor, CRIME), anderer Bundesländer, des Bundes und anderer Staaten sowie öffentlichen und anderen nicht-öffentlichen Quellen. Fließen die Daten jeweils automatisiert ein?

Die Software „hessenDATA“ führt polizeiliche Quellen in einer Analyseplattform zusammen und greift dabei automatisiert auf die drei Datenbanken POLAS (Auskunftssystem), ComVor (Vorgangsbearbeitungssystem) und CRIME-ST (Fallbearbeitungssystem) zu. Quellsysteme anderer Bundesländer, des Bundes und anderer Staaten sowie öffentlichen und anderen nicht-öffentlichen Quellen sind nicht automatisiert angebunden.

Frage 5. Hat Hessendata auch Zugriff auf Inhalte präventivpolizeilicher und strafprozessualer Ermittlungsmaßnahmen (z.B. TKÜ, WRÜ)?
Wie wird die Zweckbindung der Daten sichergestellt?

Ja, mit der Software „hessenDATA“ können Daten aus präventivpolizeilichen und strafprozessualen Ermittlungsmaßnahmen (z.B. TKÜ) im Einzelfall integriert und ausgewertet werden. Ein direkter Zugriff auf WRÜ-Daten besteht nicht und kann ebenfalls nur abhängig vom Einzelfall integriert werden.

Gemäß § 481 II StPO dürfen Polizeibehörden nach Maßgabe der Polizeigesetze personenbezogene Daten aus Strafverfahren verwenden. Diese Norm regelt die sogenannte Umwidmung der Daten und ermöglicht ihre Verwendung auf Grundlage der Gefahrenabwehrgesetze der Länder. Gem. § 20 VI HSOG werden die in Rede stehenden Daten, die im Rahmen der Verfolgung von Straftaten gewonnen und zur Abwehr von Gefahren, die mit dem Terrorismus oder der Begehung von schwerer oder Organisierter Kriminalität in Zusammenhang stehen, nach dem HSOG weiterverarbeitet.

Frage 6. Können mit Hessendata Daten von sozialen Netzwerken wie Facebook, Instagram etc. ausgewertet werden?
Falls ja, nur öffentliche oder auch geschützte Inhalte? Fließen diese Daten automatisiert ein – über den Raptor-Dienst?

Frage 7. Wie erhält Hessendata ggf. Zugriff auf nicht öffentlich einsehbare Daten von sozialen Netzwerken mit Sitz in den USA?

Fragen 6 und 7 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Software „hessenDATA“ hat keinen Zugriff auf Daten aus sozialen Netzwerken. Die in Einzelfällen in hessenDATA vorliegenden Daten aus sozialen Netzwerken wurden nach richterlichem Beschluss angefordert und durch Analysten der Hessischen Polizei in die Plattform integriert.

Frage 8. Kann die Polizei zur Nutzung in Hessendata gem. § 26 I HSOG die Übermittlung von personenbezogenen Daten aus anderen öffentlichen Datenbeständen von Bund, Länder und Kommunen verlangen? (Verfassungsschutz, Ausländerbehörden, Melderegister etc.)

Die Polizei kann im Rahmen der gesetzlichen Möglichkeiten den Zugriff auf Daten verlangen. Dabei kann es sich beispielsweise um Daten von Ausländerbehörden oder auch Melderegistern

handeln. Daten des Bundes, wie beispielsweise des Bundesamts für Verfassungsschutz, oder der Länder, wie der Landesämter für Verfassungsschutz, werden nicht genutzt.

Frage 9. Kann die Polizei zur Nutzung in Hessendata gem. § 26 I HSOG die Übermittlung von personenbezogenen Daten aus nicht-öffentlichen Datenbeständen von Unternehmen, Verbänden und Privatpersonen verlangen?
Falls ja, aus welchen?

Die Polizeibehörden können gemäß § 26 HSOG von öffentlichen Stellen oder nicht-öffentlichen Stellen zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn dies zur Abwehr der Gefahr erforderlich ist. Diese können gemäß § 25a HSOG in hessenDATA verwendet werden.

Wiesbaden, 12. Juli 2019

Peter Beuth