

**Kleine Anfrage****Torsten Felstehausen (DIE LINKE) vom 20.05.2019****Hessendata – Teil 2****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. Welche Rolle spielen die Gotham-Komponenten Raptor und Phoenix bei der Datenanalyse?
Keine. Komponenten mit diesen Bezeichnungen sind kein Bestandteil von hessenDATA.

Frage 2. Wie lange werden die Daten in Hessendata gespeichert? Kann die Einrichtung von Hessendata oder die Nutzung der Anwendungen von Hessendata Anlass zur Verlängerung der Speicherdauer gemäß § 27 IV HSOG geben?

Die Prüf- und Löschrufen der Quellsysteme werden in hessenDATA übernommen; es handelt sich um die Löschrufen aus dem HSOG.

Die Fristen betragen bei Kindern zwei Jahre, bei Jugendlichen fünf Jahre, bei Personen über siebenzig Jahre fünf Jahre und bei anderen Personen zehn Jahre.

- Frage 3. Haben Mitarbeiter von Palantir oder anderen externen Dienstleistern, die mit der Wartung, Weiterentwicklung und Anpassung von Hessendata betraut sind, Zugriff auf die Daten in Palantir oder den Quellsystemen?
Falls nein, wird dies technisch oder organisatorisch unterbunden?

Im Polizeipräsidium Frankfurt arbeitet ein polizeiliches Projektteam mit einem Team von sicherheitsüberprüften Mitarbeitern der Firma Palantir zusammen, um die Software an die Bedarfe der hessischen Polizei anzupassen. Durch verschiedene organisatorische und technische Maßnahmen wird die IT-Sicherheit gewährleistet und die Arbeit der Palantir-Mitarbeiter überwacht. So wird ein hinterlegtes Sicherheitskonzept befolgt, welches auf der Informationssicherheitsrichtlinie für die Hessische Landesverwaltung und den Vorgaben der Informationssicherheitsleitlinie für die hessische Polizei basiert. Externe Dienstleister sind nicht mit der Wartung, Weiterentwicklung und Anpassung von HessenDATA vertraut.

- Frage 4. Von wie vielen Arbeitsplätzen hessischer Sicherheitsbehörden ist der Zugriff auf Hessendata möglich und wie viele Mitarbeiter sind im System berechtigt?

Die Analyseplattform hessenDATA ist in das Netz eingebunden und bei Bedarf von jedem Arbeitsplatz in Hessen technisch erreichbar. Ein Zugriff und die Nutzung auf die gespeicherten Datensätze ist allerdings ausschließlich durch das geschulte Personal der Polizei möglich. Bislang wurden ca. 700 Mitarbeiter in der Nutzung von hessenDATA geschult, es handelt sich schwerpunktmäßig um Ermittler der Kriminalpolizei. Der Zugriff auf die Daten ist durch ein Rollen- und Rechtekonzept geregelt.

- Frage 5. Haben alle berechtigten Mitarbeiter die gleichen Leserechte? Falls nicht, nach welchen Kriterien werden die Rechte unterschieden?

Die Nutzer der Analyseplattform hessenDATA sind in verschiedene Gruppen kategorisiert, welche jeweils unterschiedliche Zugriffsrechte auf den analysierbaren, integrierten Datenbestand erhalten.

Die Einteilung der Nutzergruppen in der Analyseplattform hessenDATA erfolgt automatisiert über die Zugehörigkeit der Mitarbeiter zu ihrer Organisationseinheit. Mit diesen Gruppen und den damit verbundenen Rechten, ist der Schutz der Daten, insbesondere aus besonders schutzwürdigen Bereichen der Polizei (beispielsweise Staatsschutz) gewährleistet, ohne dabei die größtmögliche Zusammenarbeit aller Arbeitsbereiche der Analyseplattform entscheidend zu schmälern.

- Frage 6. Ist ein Zugriff auf Palantir auch von mobilen Arbeitsplätzen (z.B. Laptop, Smartphone, Tablet) möglich?

Die hessische Polizei verfügt über mobile Standardarbeitsplätze, die an das interne Polizeinetzwerk angebunden sind. Eine mobile Anwendung von hessenDATA befindet sich aktuell im Pilotbetrieb.

- Frage 7. Welche Überprüfung nach SÜG (Ü1, Ü2, Ü3) wird für Mitarbeiter von Palantir und anderen Dienstleistern, die mit der Wartung, Weiterentwicklung und Anpassung von Hessendata betraut sind, vorgenommen? Fiel die Überprüfung aller Mitarbeiter, die eingesetzt wurden und werden, positiv aus?

Die Mitarbeiter der Firma Palantir werden mittels einer Sicherheitsüberprüfung gemäß § 7 Hessisches Sicherheitsüberprüfungsgesetz (Ü1) überprüft oder verfügen über eine internationale Unbedenklichkeitsbescheinigung (sog. „SECURITY CLEARANCE“). Die Sicherheitsüberprüfung erfolgt gemäß § 10 Absatz 1 Hessisches Sicherheitsüberprüfungsgesetz durch den Geheimdienstbeauftragten des Polizeipräsidents Frankfurt am Main unter Mitwirkung des Landesamts für Verfassungsschutz. Die durchgeführten Überprüfungen der bisher eingesetzten Palantir-Mitarbeiter verliefen ohne Beanstandung.

- Frage 8. Greift Hessendata online auf die Quelldatenbanken zu oder werden die Datenbestände der Quellsysteme in Hessendata beim Import kopiert? Falls letzteres, wie wird die Konsistenz der Daten (bei Veränderung, Löschung) und die Beibehaltung der Zweckbindung sichergestellt?

Relevante Daten aus den Quelldatenbanken POLAS, ComVor und CRIME werden nach hessenDATA automatisiert übertragen. Der Datenbestand von hessenDATA wird in regelmäßigen Intervallen mit den Quelldatenbanken synchronisiert, damit wird die Beibehaltung der Löschfristen sichergestellt.

Frage 9. Laut Zwischenbericht des Untersuchungsausschusses 19/3 hat Hessendata keinen Zugriff auf das Internet. Wie gelangen Social Media Daten und Daten aus anderen Internetquellen in das System?

Die Analyseplattform hessenDATA hat keinen Zugriff auf das Internet. Die in Einzelfällen in hessenDATA vorliegenden Daten aus dem Internet, z.B. aus sozialen Netzwerken, wurden nach richterlichem Beschluss angefordert und sodann durch Analysten der Hessischen Polizei manuell in die Plattform integriert.

Wiesbaden, 12. Juli 2019

Peter Beuth