



HESSISCHER LANDTAG

21. 10. 2020

Kleine Anfrage

Dirk Gaw (AfD) und Klaus Herrmann (AfD) vom 15.09.2020

Übergabe hochsensibler Ermittlungsdaten von der hessischen Staatsanwaltschaft an externe IT-Firmen, mit ungewisser Sicherheitsüberprüfung

und

Antwort

Ministerin der Justiz

Vorbemerkung Fragesteller:

Bei Ermittlungen müssen Staatsanwaltschaften schon seit geraumer Zeit private Dienstleister mit der Überprüfung beziehungsweise Auswertung von hochsensiblen Ermittlungsdaten beschäftigen.

Das ist einleuchtend, wenn man bedenkt, dass teilweise große Datenmengen von sichergestellten Computerfestplatten und Handyspeichern ausgelesen werden. Es stellt sich die Frage, wer diese Daten auswertet. Nach Medienberichten der Hessenschau, haben Staatsanwälte empfindliche Daten, die mit dem Bereich Kinderpornographie, Betrug und Geldwäsche in Zusammenhang stehen, an externe IT-forensische Unternehmen übergeben, ohne eine Überprüfung der Angestellten einzufordern. Weder Führungszeugnisse noch polizeiliche Informationen wurden im Vorfeld verlangt.

Somit könnte es im schlimmsten Fall passieren, dass Vorbestraften durch ihre Anstellung bei einem solchen Unternehmen, die Verantwortung für die Verarbeitung von Daten übertragen wird, für die sie nicht geeignet sind, oder die Daten gar missbrauchen. Auch der Vorsitzende des Bundes Deutscher Kriminalbeamter (BDK) Hessen sieht hier eine erhebliche Sicherheitslücke.

Es ist nicht auszudenken, was passieren könnte, wenn beispielsweise ein, wegen pädosexueller Straftaten Verurteilter, über sein Anstellungsverhältnis, mit der Auswertung kinderpornographischer Daten befasst werden würde. (Quelle: Hessenschau vom 23.08.2020)

Diese Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

- Frage 1. Werden die von Polizei und Staatsanwaltschaft mit der Überprüfung beauftragten externen Dienstleister und ihre Mitarbeiter regelmäßig sicherheitsüberprüft, oder handelt es sich um eine einmalige Sicherheitsüberprüfung?
- Frage 2. Falls es sich um eine einmalige Sicherheitsüberprüfung handeln sollte, wie bewertet die Hessische Landesregierung diese mögliche Sicherheitslücke in der Datenweitergabe und ist zukünftig generell eine Sicherheitsüberprüfung externer Dienstleister und Mitarbeiter geplant?
- Frage 3. Ist es zutreffend, dass die Polizei oder die Staatsanwaltschaft ermittlungsrelevante Daten an dafür spezialisierte Firmen weitergibt, ohne eine Sicherheitsüberprüfung der mit der Auswertung der Datenträger und Daten beschäftigten Mitarbeiter durchzuführen? Findet die Einholung des polizeilichen Führungszeugnisses statt?

Die Fragen 1. bis 3. werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Die Entscheidung über die Beauftragung eines Sachverständigen in einem Ermittlungsverfahren steht nach Maßgabe der Bestimmungen der § 161 Abs. 1 Satz 1 und § 73 StPO im Ermessen der Staatsanwältin bzw. des Staatsanwalts. Die Zuziehung von Sachverständigen ist dann notwendig, wenn die eigene Sachkunde der Staatsanwältin bzw. des Staatsanwalts und im späteren Verlauf des Strafverfahrens des Gerichts zur Beurteilung anstehender Fragen nicht ausreicht, weil es auf besondere Sachkunde ankommt.

Wie in den anderen Ländern werden auch in Hessen Sachverständige beauftragt, denen dann die zur Erfüllung des Sachverständigenauftrags notwendigen Daten zugänglich gemacht werden müssen. In den Bereichen Kinderpornografie, Betrug und Geldwäsche setzen hessische Staatsanwaltschaften weit überwiegend Sachverständige von zwei bundesweit tätigen Unternehmen mit Sitz im Freistaat Bayern ein.

Die Sachverständigen beider Unternehmen sind auf der gemäß Nr. 70 Abs. 3 der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) von der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) geführten Liste bewährter EDV-Sachverständiger aufgeführt.

Für die Aufnahme auf die Liste bewährter EDV-Sachverständiger müssen Unternehmen hohe Anforderungen erfüllen. Neben dem Nachweis besonderer Sachkunde, Referenzen und Zuverlässigkeit gelten eingehende technische Anforderungen für die Lagerung, den Transport, die Sicherheit der asservierten Datenträger, die IT-Sicherheit der Datennetze sowie Verpflichtungen zur Wahrung von Geheimhaltung und Datenschutz.

Nicht auf der Liste befindliche Sachverständige haben vor der Vergabe von Gutachtaufträgen eine Verpflichtungserklärung auf das Datengeheimnis nach § 53 des Bundesdatenschutzgesetzes (BDSG) abzugeben, nach der es, auch nach Beendigung des Auftragsverhältnisses untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Zugleich werden diese über die Strafbarkeit von Verstößen gegen das Datengeheimnis belehrt. Die externen Sachverständigen haben zudem zu gewährleisten, dass alle mit der Bearbeitung oder Erfüllung des Gutachtauftrages betrauten Personen die gesetzlichen Bestimmungen über den Datenschutz beachten (Datengeheimnis nach § 53 BDSG).

Für die Einführung verpflichtender Überprüfungen fehlt es an einer Rechtsgrundlage. Gerichtlich oder von Seiten der Staatsanwaltschaft zu bestellende Sachverständige fallen in den Schutzbereich der Berufsfreiheit nach Artikel 12 des Grundgesetzes. Sie üben diesen Beruf auf Dauer aus und leben von dem Lohn der Sachverständigentätigkeit. Art. 12 Abs. 1 Satz 2 des Grundgesetzes erlaubt Eingriffe in die Berufsfreiheit nur auf Grundlage einer gesetzlichen Regelung.

Frage 4. Wenn Frage 3 mit ja beantwortet wird, stellt in diesem Fall die Weitergabe von Datenträgern und Daten zur Sicherung und Auswertung einen Verstoß gegen die DSGVO dar?

Frage 5. Wenn Frage 4 mit ja beantwortet wird, welche konkreten Haftungs- bzw. Schadensersatzansprüche ergeben sich hieraus?

Die Fragen 4. bis 5. werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Die Datenschutzgrundverordnung ist nach ihrem Artikel 2 Abs. 2 Buchst. d) auf die Verarbeitung personenbezogener Daten im Strafverfahren nicht anwendbar.

Frage 6. Besteht die Möglichkeit, dass alle Personen, deren personenbezogene Daten (Bilder, Kontaktdaten, etc.) im Rahmen der Ermittlungen durch diese IT-Firmen und deren Mitarbeiter ausgewertet bzw. verarbeitet werden, über potenzielle Verstöße hinsichtlich der Datenverarbeitung informiert werden?

Betroffene von Verstößen haben ein weitgehendes Akteneinsichtsrecht.

Frage 7. Können Personen, deren Computer, Mobiltelefon oder sonstige Datenträger zur Auswertung beschlagnahmt bzw. sichergestellt wurden, von der Polizei oder der Staatsanwaltschaft eine Auskunft über das Ausmaß der Datenweitergabe verlangen?

Ja (§ 147 StPO bzw. §§ 103, 475 StPO und § 57 BDSG).

Frage 8. Sieht die Landesregierung Anhaltspunkte dafür, dass die Möglichkeit besteht, dass aufgrund mangelnder Sicherheitsüberprüfung, Mitarbeiter der IT-Firmen trotz einschlägiger Straffälligkeit ermittlungsrelevante Daten verarbeitet haben?

Nein.

Frage 9. Wenn Frage 8 mit Ja beantwortet wird, kann ausgeschlossen werden, dass diese Daten nicht missbräuchlich verwendet wurden, beispielsweise durch Weitergabe an Dritte?

Entfällt.

Frage 10. Wird die Landesregierung Maßnahmen einleiten, um künftig die Datenweitergabe an externe IT-Firmen sicher zu gestalten?

Angesichts der oben beschriebenen Maßnahmen und Strafdrohungen bei Verstößen besteht aus Sicht der Landesregierung derzeit kein Handlungsbedarf.