

ANTWORT

zu der

Anfrage des Abgeordneten Michael Hilberer (PIRATEN)

betr.: Schutz privater Daten bei Polizeikontrollen

Vorbemerkung des Fragestellers:

„Am Morgen des 19.07.2013 wurde der Abgeordnete im Abgeordnetenhaus Berlin, Andreas Baum nach eigenen Angaben von Zivilbeamten kontrolliert, als er gerade sein Motorrad besteigen wollte. Neben ihm sei auch ein Radfahrer überprüft worden, der gerade sein Smartphone nutzte und, Baums Eindruck nach, das eigentliche Ziel der Kontrolle gewesen sei. Nachdem ein Beamter auch Baum gründlich durchsucht hatte, habe der Polizist ihn um die Herausgabe seines Smartphones gebeten, um feststellen zu können, ob dieses gestohlen sei. Dieser habe ihm im Rahmen der Aufforderung versichert: „Ich werde schon nicht in Ihren Nachrichten rumgucken, oder haben Sie etwas zu verbergen?“ So zitiert Andreas Baum den Polizeibeamten auf seiner privaten Homepage www.andreasbaum.info.

Nach längerer Wartezeit habe Baum nach Rückgabe des Handys bemerkt, dass zuletzt das SMS-Programm und das normale Telefon benutzt worden seien. Er selbst allerdings hätte als letztes andere Programme benutzt, woraus er folgerte, dass die Polizisten diese Anwendungen geöffnet haben müssen. Auf diese Feststellung von Baum angesprochen, habe ein Beamter ihm entgegnet: „Es kann schon einmal vorkommen, dass man beim Rumtippen da drauf kommt.“

Bei einer späteren Überprüfung der Anwendungen wurde klar, dass Telefon- und SMS-Daten bis zurück in das Jahr 2011 aufgerufen wurden.“

Vorbemerkung Landesregierung:

Der geschilderte Vorfall ist der Landesregierung nur durch die Anfrage des MdL Hilberer sowie die Berichterstattung bekannt. Insbesondere liegen hier keine Informationen über die Hintergründe des beschriebenen Vorgangs vor.

Die nachfolgenden Antworten der Landesregierung beziehen sich – soweit nichts anderes angegeben ist - ausschließlich auf saarländisches Landesrecht und sind insofern nicht auf den in der Vorbemerkung des Fragestellers geschilderten Vorgang übertragbar.

Aufgrund welcher Rechtsgrundlage und unter welchen weiteren rechtlichen Voraussetzungen kann die Polizei im Saarland Mobiltelefone im Rahmen von allgemeinen Polizeikontrollen oder Verkehrskontrollen ohne konkreten Tatverdacht gegen die betreffende Person, die das Handy mit sich führt, durchsuchen?

Zu Frage 1:

Es gibt keine Rechtsgrundlage welche die Vollzugspolizei des Saarlandes ermächtigt, Mobiltelefone im Rahmen von allgemeinen Polizeikontrollen oder Verkehrskontrollen ohne konkreten Tatverdacht zu durchsuchen. Der Anwendungsbereich der Strafprozessordnung (StPO) ist erst eröffnet, wenn gegen eine (bekannte oder unbekannte) Person ein Ermittlungsverfahren (und sei es auch nur konkludent) eingeleitet worden ist, weil gegen sie der (Anfangs-) Verdacht der Begehung einer Straftat besteht (§ 152 Absatz 2 StPO). Auch Durchsuchungen beim Verdächtigen und anderen Personen (§§ 102, 103 StPO) setzen stets das Vorhandensein eines Anfangsverdachts und – hiermit einhergehend - einen „Beschuldigten“ voraus.

Nach dem Polizeirecht sind intensive Grundrechtseingriffe erst ab einer bestimmten Verdachts- beziehungsweise Gefahrenstufe zulässig.

In welchem konkreten Umfang ist eine solche Durchsuchung zulässig?

- a) Darf im Rahmen dieser Durchsuchung die IMEI des Mobiltelefons festgestellt werden?
Wenn ja, unter welchen Voraussetzungen?
- b) Darf darüber hinaus auch auf andere auf dem Handy gespeicherte Daten wie Adressbücher, SMS/sonstige digitale Kurznachrichten (Whatsapp usw.), Anruflisten, Verbindungsdaten, Fotos, Videos, Social Networking Daten oder sonstige Apps zugegriffen werden?
Wenn ja, unter welchen Voraussetzungen?

Zu Frage 2:

Siehe Antwort zu Frage 1. Eine Durchsuchung durch die Polizei im Rahmen der Gefahrenabwehr wäre allenfalls unter den Voraussetzungen des § 18 des Saarländischen Polizeigesetzes (SPoIG) möglich.

Danach ist die Durchsuchung einer Sache dann zulässig, wenn sie von einer Person mitgeführt wird, die selbst durchsucht werden darf oder Tatsachen die Annahme rechtfertigen, dass sich in ihr

- a. eine hilflose Person befindet oder
- b. eine andere Sache befindet, die sichergestellt werden darf.

Die Durchsuchung von Mobiltelefonen muss sich zudem an den Vorgaben des Bundesverfassungsgerichts zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG 120, 274) orientieren. Das Bundesverfassungsgericht hat mit Urteil vom 27. Februar 2008 aus dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet, das den Einzelnen vor heimlichem staatlichen Zugriff auf sein von ihm betriebenes IT-System schützen soll. Zu solchen informationstechnischen Systemen gehören auch sämtliche Mobiltelefone und elektronischen Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

Zu Frage 2 a):

Nein, siehe Antwort zu Frage 1.

Zu Frage 2 b):

Nein, siehe Antwort zu Frage 1.

Gab es auch im Saarland Fälle, in denen saarländische Polizisten im Rahmen von Personen- oder Verkehrskontrollen auf Daten, die auf dem Handy gespeichert sind, zugegriffen haben?

- a) Wenn ja, in wie vielen Fällen?
- b) Aus welchen Anlässen wurden jeweils diese Durchsuchungen der gespeicherten Inhalte durchgeführt?

Zu den Fragen 3 a) und 3 b):

Siehe Antwort zu Frage 1. Solche Fälle sind der Landesregierung folglich auch nicht bekannt.

In welcher Form werden die gesichteten Daten erfasst?

- a) Werden diese in digitaler Form gespeichert oder deren Inhalte aktenmäßig festgehalten?
Wenn ja, in welcher Form genau?
- b) Wie lang ist die maximale Speicherdauer für die gesicherten Daten?

Zu den Fragen 4 a) und 4 b):

Siehe Antwort zu Frage 1. Es werden im Rahmen von allgemeinen Personen- oder Verkehrskontrollen keine Daten i. S. d. Fragestellung erfasst und gespeichert.

Setzt die saarländische Polizei spezialisierte Hardware zum Auslesen der Daten von Mobiltelefonen ein?

- a) Wenn ja, können mit diesen Geräten Daten auf gelockten SIM-Karten extrahiert werden, indem man sich vom Netzbetreiber einfach die PUK geben lässt?

Zu Frage 5:

Für allgemeine Personen- und Verkehrskontrollen auf Grundlage des allgemeinen Polizeirechts gilt das eingangs zu Frage 1 Ausgeführte.

Eine forensische Untersuchung von Mobiltelefonen ist zu repressiven Zwecken unter Beachtung der gesetzlichen Vorgaben der StPO möglich. Hierfür ist speziell entwickelte Hard- und Software erforderlich.

Zu Frage 5 a):

Soweit ohne PIN/ PUK die Auswertung von Mobiltelefonen nicht möglich ist, wird seitens der IT-Forensik bei der beauftragenden sachbearbeitenden Dienststelle eine Anfrage beim Provider unter den gesetzlichen Vorgaben und Beachtung der verfassungsmäßigen Schranken angeregt.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Im Falle der Strafverfolgung sind die jeweiligen gesetzliche Eingriffsermächtigungen in den §§ 94, 98, 100a ff., 102, 103, 110 Strafprozessordnung (StPO) geregelt. Diese entsprechen der vor allem für das Recht auf informationelle Selbstbestimmung geltenden Vorgabe, wonach der Gesetzgeber den Verwendungszweck der Daten bereichsspezifisch, präzise und für den Betroffenen erkennbar bestimmen muss. Dem wird durch die strenge Begrenzung aller Maßnahmen auf den Ermittlungszweck genüge getan. Im Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (Gesetz vom 20.06.2013, BGBl. I S. 1602) hat der Gesetzgeber durch die nunmehr geltende Fassung des § 100j StPO sichergestellt, dass kein heimlicher Zugriff auf Daten des Betroffenen ohne richterliche Zustimmung erfolgt. Grundsätzlich gilt für diese Maßnahmen ein Richtervorbehalt, bei Gefahr im Verzug besteht allerdings für die Staatsanwaltschaft und deren Ermittlungspersonen ein Anordnungsrecht, das einer nachträglichen richterlichen Bestätigung bedarf.

Welche Maßnahmen trifft die Landesregierung, um den sensiblen Kernbereich der privaten Lebensführung bei Polizeikontrollen zu schützen?

- a) Gibt es spezielle „Awareness-Programme“ oder Vergleichbares, um Polizeibeamte für die besondere Schutzwürdigkeit der heute auf Mobiltelefonen gespeicherten Daten zu sensibilisieren?

- b) Gibt es Dienstanweisungen oder Ähnliches, um die neue technische Qualität des Eingriffs in die Privatsphäre bei der Kontrolle von Mobiltelefonen zu minimieren?

Zu Frage 6:

Ein Eingriff in den grundrechtlich geschützten und durch die verfassungsgerichtlichen Vorgaben hinreichend definierten Kernbereich wäre im Rahmen allgemeiner Polizeikontrollen nur in Form eines Rechtsverstoßes denkbar. Dem wird allerdings durch intensive Aus- und Weiterbildung der Vollzugspolizeibeamtinnen und –beamten vorgebeugt.

Zu Frage 6 a):

Unabhängig davon wären spezielle „Awareness-Maßnahmen“ grundsätzlich eine Möglichkeit, eine Sensibilisierung von Polizeibeamten im Hinblick auf die Schutzwürdigkeit von Daten auf Mobiltelefonen zu erreichen. Es handelt sich jedoch bei der in Rede stehenden Thematik letztlich um die Kenntnis und Anwendung von Rechtsvorschriften unter besonderer Berücksichtigung des verfassungsrechtlich garantierten Rechts auf informationelle Selbstbestimmung.

Die rechtlichen Grundlagen wiederum werden im Rahmen der polizeilichen Aus- und Fortbildung, zum Beispiel an der Fachhochschule für Verwaltung, intensiv und aus Sicht der Landesregierung hinreichend behandelt.

Zu Frage 6 b):

Zu der in Rede stehenden Thematik gibt es im Landespolizeipräsidium keine Dienstanweisungen oder sonstige Verwaltungsvorschriften.

Es konnte bislang keine Notwendigkeit dafür erkannt werden, die entsprechenden gesetzlichen Vorschriften durch Gesetzesauslegung oder normkonkretisierende Erwägungen zu ergänzen.