STAATSMINISTERIUM
DER JUSTIZ

Freistaat
SACHSEN

Die Staatsministerin

SÄCHSISCHES STAATSMINISTERIUM DER JUSTIZ
Hospitalstraße 7 | 01097 Dresden

Präsidenten des Sächsischen Landtages
Herrn Dr. Matthias Rößler
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Durchwahl
Telefon +49 351 564 15000
Telefax +49 351 564 15009

Staatsministerin@
smj.justiz.sachsen.de*

Aktenzeichen
(bitte bei Antwort angeben)
1040E/46/136-KLR

Dresden,
25. Februar 2020

Kleine Anfrage des Abgeordneten Rico Gebhardt (DIE LINKE)
Drs.-Nr.: 7/1296
Thema: Volatilität digitaler Daten und (fehlende) Standards sowie fachliche Qualifikation zur Überprüfung der Zuverlässigkeit und des Beweiswertes digitaler Beweismittel durch Ermittlungspersonen, Richter, Staatsanwälte und Rechtsanwälte im Strafverfahren

Sehr geehrter Herr Präsident,

den Fragen sind folgende Ausführungen vorangestellt:

„In einer Parlamentarischen Anfrage von Abgeordneten des Europaparlaments zur schriftlichen Beantwortung an die Europäische Kommission (E-002673-19) wird festgestellt:

‚Am 18. August 2019 kündigten die dänischen Behörden an, dass 10 700 Entscheidungen von Strafgerichten, die seit 2012 ergangen sind, wegen Fehlern in den Trackingdaten in der Telekommunikation, die als Beweismittel verwendet wurden, überprüft werden sollen. Die Probleme, die zum Teil auf die IT-Systeme der Polizei und zum Teil auf Telekommunikationssysteme zurückzuführen sind, führten zu einem zweimonatigen Verbot der Nutzung von Telekommunikationsdaten durch Staatsanwälte. In dieser Zeit sollen die Fehler und die möglichen Folgen untersucht werden.'“

Namens und im Auftrag der Sächsischen Staatsregierung beantworte ich die Kleine Anfrage wie folgt:

JOB MIT J?
JUSTIZVOLLZUGSBEAMTE
WWW.JOB-MIT-J.DE

Hausanschrift:
Sächsisches Staatsministerium der Justiz
Hospitalstraße 7
01097 Dresden

Briefpost über Deutsche Post
01095 Dresden

www.justiz.sachsen.de/smj

Verkehrsverbindung:
Zu erreichen mit
Straßenbahnlinien
3, 6, 7, 8, 11

Parken und behindertengerechter Zugang über Einfahrt Hospitalstraße 7

Hinweise zum **Datenschutz** erhalten Sie auf unserer Internetseite. Auf Wunsch senden wir Ihnen diese Hinweise auch zu.

*Kein Zugang für elektronisch signierte sowie für verschlüsselte elektronische Nachrichten; nähere Informationen zur elektronischen Kommunikation mit sächsischen Justizbehörden unter www.justiz.sachsen.de/E-Kommunikation.

Frage 1:
Welche Probleme sind der Staatsregierung hinsichtlich mangelnder Zuverlässigkeit digitaler Beweismittel insbesondere (aber nicht nur) aus Smartphones, TKÜ und Funkzellen-Abfragen sowie bezüglich fehlender Standards zur Feststellung derselben im Rahmen des strafrechtlichen Erkenntnisverfahrens, besonders während der Beweisaufnahme in der strafrechtlichen Hauptverhandlung, im Bereich der sächsischen Justiz bekannt?

Im Rahmen der Ermittlungstätigkeit als auch bei den Gerichten sind bisher keine Probleme im Zusammenhang mit mangelnder Zuverlässigkeit elektronischer Beweismittel bekannt geworden. Auch Probleme wegen fehlender Standards zur Feststellung digitaler Beweismittel sind nicht bekannt.

Zur Klärung technischer Fragen zum Beweiswert und zu der Aussagekraft der elektronischen Daten besteht bei allen sächsischen Staatsanwaltschaften und bei der Generalstaatsanwaltschaft die Möglichkeit der Beratung durch den Referenten für IT-Forensik. Diesen ist bekannt, dass bestimmte Daten, wie Dateisystem-Zeitstempel und Geo-Daten, besonders zu betrachten und auf Plausibilität zu prüfen sind. Die Referenten für IT-Forensik sind auch in der Lage zu überprüfen, ob die Herkunft der Daten in der Akte ausreichend dokumentiert sind. Im Rahmen der Hauptverhandlung besteht zudem die Möglichkeit für das Gericht, welchem im Rahmen der Beweiswürdigung auch die Bewertung der Qualität digitaler Beweismittel obliegt, insbesondere den Polizeibeamten oder Referent/innen für IT-Forensik, die die Sicherung oder Auswertung der Daten durchgeführt hat, als Zeug/innen bzw. sachverständigen Zeug/innen zu vernehmen.

Frage 2:
Welche Standards werden in der digitalen Forensik und in der Strafjustiz Sachsens bei der Herstellung und Verarbeitung digitaler Beweise zu Grunde gelegt? (Bitte die Rechtsgrundlagen, technischen Standards, Leitfäden, operativen Anweisungen etc., welche entsprechende Standards und Kriterien vorgeben, für die beteiligten Berufsgruppen benennen.)

Telekommunikationsüberwachungs- (TKÜ) und Funkzellendaten werden auf der Grundlage der §§ 100a, 100g StPO erhoben. Rechtsgrundlage für die Datengewinnung aus elektronischen Geräten des Beschuldigten sind die §§ 102, 110 Abs. 1 StPO. Rechtsgrundlage für die Durchsicht von Daten in Clouddiensten, die mit den elektronischen Geräten des Beschuldigten verbunden sind, ist § 110 Abs. 3 StPO.

Die technischen Standards der Sicherung und Auswertung elektronischer Daten werden jeweils durch die verwendete Hard- und Software vorgegeben, wobei eine Zertifizierung nicht vorliegt.

Die Sicherung und Auswertung elektronischer Datenträger erfolgt in der Regel durch die Polizei. Dort erfolgt die Verarbeitung erhobener, beweiserheblicher digitaler Daten auf Antrag der ermittlungsführenden Stelle nach festgelegten Prinzipien und Arbeitsroutinen unter Nutzung der zur Verfügung stehenden technischen Möglichkeiten. Dabei werden forensische Untersuchungen grundsätzlich nicht an der Originaldatei (Urkopie) vorgenommen. Diese bleibt bis zum Ende des Strafverfahrens unverändert. Ausnahmen bilden allein Maßnahmen zum Schutz des Kernbereichs privater Lebensgestaltung sowie zum Schutz von Berufsgeheimnisträgern im Rahmen von Überwachungsmaßnahmen.

Die technischen Vorgänge werden in der Akte dokumentiert und können von allen Beteiligten des Strafverfahrens nachvollzogen werden. Die elektronischen Daten werden als Beweismittel zu dem jeweiligen Verfahren asserviert. In Einzelfällen erfolgen bei den Staatsanwaltschaften die Sicherung und die Auswertung der elektronischen Daten durch die/den Referent/in für IT-Forensik. Die von diesem genutzte Hard- und Software wurde unter Beachtung der Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschafft. Die Referent/innen für IT-Forensik verwenden den „Leitfaden IT-Forensik“ des BSI, der die grundlegenden Standards der IT-Forensik beschreibt.

Soweit Telekommunikationsdaten durch Telekommunikationsdienstleister sichergestellt und übermittelt werden, sind die dafür erforderlichen technischen Einrichtungen gemäß § 110 TKG durch die Telefondienstleister vorzuhalten. Danach legt die Bundesnetzagentur technische Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Auskunftserteilung sowie zur Ge-

staltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie fest. Dabei sind internationale technische Standards zu berücksichtigen. Eine Überwachung erfolgt durch die Bundesnetzagentur.

Die Hersteller technischer Einrichtungen zur Umsetzung von Überwachungsmaßnahmen können von der Bundesnetzagentur verlangen, dass sie diese Einrichtungen im Rahmen einer Typmusterprüfung im Zusammenwirken mit bestimmten Telekommunikationsanlagen daraufhin prüft, ob die rechtlichen und technischen Vorschriften der Telekommunikations-Überwachungsverordnung und der o. g. Technischen Richtlinie erfüllt werden.

Frage 3:
Inwieweit sind das GKDZ (bzw. bis zu dessen voller Arbeitsfähigkeit das LKA) und die LIT in die Erarbeitung und Vermittlung (Training) von Standards zur Sicherung der Zuverlässigkeit der Methoden bei der Verarbeitung und Analyse von Daten aus Telekommunikationssystemen entlang der Verwahrkette (Chain of Custody) vom Telekommunikationsanbieter/ Netzbetreiber bis zur Einreichung als digitale Beweise vor Gericht einbezogen?

Aufgrund der in der Beantwortung der Frage 2 ausgeführten Vorgehensweise ist die Teilnahme des Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizei der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts (GKDZ AöR), welches sich derzeit noch in der Aufbauphase befindet, an der Erarbeitung von Standards für die Erfassung und Übermittlung dieser Daten an die berechtigten Stellen – jedenfalls soweit es die Telekommunikationsüberwachung und Verkehrsdatenerhebung betrifft – entbehrlich. Die LIT ist in die Erarbeitung und Vermittlung der vorgenannten Standards nicht eingebunden.

Frage 4:
Wie wird gegenwärtig die erforderliche fachliche Qualifikation von Ermittlungspersonen sowie von Strafjuristen (Richtern, Staatsanwälten, Rechtsanwälten), die

für die Prüfung der Zulässigkeit und des Beweiswertes von digitalen Beweismitteln erforderlich ist (insbesondere von Smartphone-Daten, TKÜ- und Funkzellen-Daten), durch Maßnahmen der Staatsregierung gesichert? (Bitte die konkreten Maßnahmen für die verschiedenen Berufsgruppen gesondert benennen.)

Frage 5:
Welche Vorkehrungen trifft die Staatsregierung, insbesondere das Staatsministerium für Inneres und das Sächsische Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung für die Zukunft, um die notwendigen rechtliche Regelungen und (technischen) Standards für digitale Forensik und zur Überprüfung digitaler Beweise in der Beweisaufnahme im Strafverfahren zu schaffen und die am Strafverfahren beteiligten Richter, Staatsanwälte und Rechtsanwälte für den Umgang mit digitalen Beweismitteln zu qualifizieren?

Zusammenfassende Antwort auf die Fragen 4 und 5:

Im *Bereich der sächsischen Polizei* findet die fachliche Qualifizierung von Ermittlungspersonen sowie von IT-Spezialisten im Rahmen der zentralen Fortbildung durch die Bildungsträger der sächsischen Polizei entsprechend des Fortbildungskataloges sowie dezentral im Bundesgebiet statt. Je nach Einsatzbereich werden Polizeivollzugsbeamtinnen und -beamte auf Grundlage dahingehender bundeseinheitlichen Aus- und Fortbildungskonzepte geschult. Dabei unterliegen die Lehrinhalte einer ständigen Fortschreibung an aktuelle Bedarfe.

Das Polizeiverwaltungsamt hat dabei im vergangenen Jahr folgende zentrale Fortbildungen angeboten:

- Sicherstellung von Datenverarbeitungsanlagen und Datenträgern,
- Internet-Grundlagen und Nutzungsmöglichkeiten,
- Nutzung des Internets für polizeiliche Ermittlungen,
- Nutzung des Internets bei der Bekämpfung der Informations- und Kommunikations-Kriminalität (IuK-Kriminalität),
- Methodik der Auswertung digitaler Spuren,
- IT – Grundmodul für polizeiliche Sachbearbeiter als Ersteinschreiter

- Betriebssystem Windows – Aufbaumodul 2,
- Betriebssystem Windows (Client-/Serverkomponenten) – Aufbaumodul 3,
- Internet-Grundmodul für polizeiliche Sachbearbeiter als Ersteinschreiter,
- IuK-Tatortarbeit/Sachbearbeitung,
- Datensicherung/IuK-Beweissicherung (Tatortarbeit) – Aufbaumodul 1,
- IuK-Recht – Grundmodul,
- IuK-Recht – Aufbaumodul 1,
- Betriebssystem Unix/Linux – Grundmodul,
- Betriebssystem Unix/Linux – Aufbaumodul,
- Netzwerke – Grundmodul,
- Manipulation in Netzwerken,
- Überblick über mobile Endgeräte.

In der Ausbildung der Laufbahngruppe 2, erste Einstiegsebene, Fachrichtung Polizei (LG 2.1 Pol) werden in den vorgesehenen Lehrkomplexen „Straftaten im Zusammenhang mit dem Internet; Betrugsdelikte; Geldwäsche“ sowie „Datenerhebung und -verarbeitung durch die Polizei“ rechtliche, taktische und technische Grundlagen vermittelt. Ferner wird ein Wahlpflichtmodul „Cybercrime“ angeboten.

Seit 2015 bietet die Hochschule der Sächsischen Polizei (FH) zudem die Sonderlaufbahn Computer- und Internetkriminalitätsdienst (CuIKD) mit dem Ziel der zügigen Akquise spezieller IT-Fachkenntnisse für die sächsische Polizei an. Hierfür sollen Absolventinnen und Absolventen eines Bachelor- oder vergleichbaren Diplomstudiengangs an einer Fachhochschule im IuK-Bereich gewonnen werden, die als Polizeivollzugsbeamte mit IuK-Spezialkenntnissen eingesetzt werden können. Im Rahmen eines verkürzten Vorbereitungsdienstes sollen diese Bediensteten die für die Aufgabenerfüllung notwendigen polizeilichen Kenntnisse und Fähigkeiten vermittelt bekommen, die sie befähigen, vollzugspolizeiliche Aufgaben der LG 2.1 Pol im Schwerpunkt CuIKD wahrzunehmen.

Des Weiteren kooperiert die sächsische Polizei mit der Hochschule Mittweida, wo aktuell ein Beamter den berufsbegleitenden Studiengang IT-Forensik/Cybercrime absolviert.

Die Komplexität der digitalen Forensik sowie deren Dynamik hinsichtlich des permanenten Hinzutretens neuer Ermittlungsmethoden/-technologien machen es erforderlich, dass in diesem Bereich ausschließlich durch die o. g. Aus- und Fortbildungsmaßnahmen geschultes Fachpersonal eingesetzt wird. Zur Sicherung der Beweisführung wird zudem im zunehmenden Maße auch externe Expertise (u. a. Gutachter) im Ermittlungsverfahren hinzugezogen. Um das hohe Maß an Transparenz und Nachvollziehbarkeit auch im gesamten Strafverfahren für alle Prozessbeteiligten zu gewährleisten, werden Ermittlungspersonen und IT-Spezialisten der sächsischen Polizei immer häufiger in Verhandlungen bei Amts- und Landgerichten als Sachverständige bzw. sachverständige Zeuginnen oder Zeugen vorgeladen.

Für die erforderliche fachliche Qualifikation von *sächsischen Richterinnen / Richtern und Staatsanwältinnen / Staatsanwälten* finden regelmäßig eine Vielzahl von Fortbildungsveranstaltungen an der Deutschen Richterakademie (DRA) und landeseigene Fortbildungsveranstaltungen zu den vorgenannten Themenbereichen statt, die sich u.a. auch mit strafprozessualen Rechtsfragen im Zusammenhang mit digitalen Beweismitteln befassen.

Das Fundament der Aus- und Fortbildung im Bereich Cyberkriminalität in Sachsen bildet eine im Jahr 2018 eingeführte flächendeckende Grundqualifizierung der Staatsanwältinnen / Staatsanwälte, die konzeptionell auf einen großen Teilnehmerkreis und eine praxisbezogene Wissensvermittlung in kurzer Zeit vor Ort ausgerichtet ist. Die Fortbildungsinhalte der Grundqualifizierung wurden in sechs Module zu je vier Stunden gegliedert. Dies ermöglicht es, die Fortbildungen flexibel nach den individuellen Anforderungen der täglichen Dezernatsarbeit wahrzunehmen und regelmäßig noch das Tagesgeschäft vor Ort wahrzunehmen. Gleichzeitig wird damit auch Teilzeitkräften Gelegenheit gegeben, ohne Zusatzaufwand an den Schulungen teilzunehmen. Inhaltlich befassen sich die aufeinander aufbauenden Module mit den technischen Grundlagen und Funktionsweise (u.a. Hardware und Betriebssysteme, Internet, Überblick Darknet, Zahlungsdienste im Internet, internetgestützte und mobilfunkgestützte Kommunikation, soziale Netzwerke), Cyberkriminalität und ihre Erscheinungsformen, Eingriffsmaßnahmen und ihre Rechtsgrundlagen (u.a. Datenarten, Überwachungsmaßnahmen) und Ermittlungsmethoden und technische Hilfsmittel (u.a. Auswertungsmöglichkeiten von Datenträgern).

Daneben werden spezielle Fortbildungen für Staatsanwältinnen / Staatsanwälte zu Ermittlungsmethoden im Internet und digitalen Beweismitteln durch die bei der Generalstaatsanwaltschaft im März 2016 neu errichtete Sächsische Zentralstelle zur Bekämpfung von Cybercrime (ZCS) angeboten.

Zudem besteht auch im Bereich der Fortbildung für Richterinnen / Richter und Staatsanwältinnen / Staatsanwälte bereits seit mehreren Jahren eine Zusammenarbeit mit der Hochschule Mittweida. So wurden in vergangenen Jahren mehrfach Fortbildungsveranstaltungen zur Kriminalitätsentwicklung im Internet einschließlich ihrer Aufdeckungs- und Nachweismöglichkeiten durch IT-gestützte Ermittlungsmethoden an der Hochschule durch deren Dozenten durchgeführt. Die Zusammenarbeit wurde im Jahr 2017 durch eine Kooperationsvereinbarung zwischen dem damaligen Sächsischen Staatsministerium der Justiz, dem Sächsischen Staatsministerium des Inneren und der Hochschule Mittweida institutionalisiert.

Ferner wird seit vergangenem Jahr erstmals eine landeseigene Tagung zum Thema „Allgemeine Ermittlungen in Strafsachen" angeboten, die u.a. auch Ermittlungen in Sozialen Medien, Auskunftsansprüche und damit verknüpfte Beweisschwierigkeiten zum Gegenstand hatte.

Schließlich besteht die Möglichkeit für sächsische Staatsanwältinnen / Staatsanwälte, sich für Fortbildungen der Agentur der Europäischen Union für Aus- und Fortbildung auf dem Gebiet der der Strafverfolgung (CEPOL) zu bewerben, die eine Vielzahl von Veranstaltungen zu speziellen Ermittlungsmaßnahmen im Zusammenhang mit digitalen Beweismitteln anbietet.

Im Hinblick auf *Rechtsanwältinnen / Rechtsanwälte* werden seitens des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung keine Maßnahmen getroffen, welche dazu dienen, deren fachliche Qualifikation im Hinblick auf die Prüfung der Zulässigkeit und des Beweiswertes von digitalen Beweismitteln sicherzustellen. Ob diesbezüglich anderweitige Maßnahmen, etwa der berufsständischen Organisationen der Rechtsanwaltschaft, durchgeführt werden, kann durch die sächsische Staatsregierung nicht beantwortet werden. Der Staatsregierung liegen hierzu keine entsprechenden Erkenntnisse vor. Die Staatsregierung ist dem Landtag nur

für ihre Amtsführung verantwortlich. Sie ist daher nur in solchen Angelegenheiten zur Auskunft verpflichtet, die in ihre Zuständigkeit fallen und muss nicht auf Fragen eingehen, die außerhalb ihres Verantwortungsbereichs liegen. Letzteres ist hier der Fall, denn die Frage betrifft ausschließlich Sachverhalte, die von den Rechtsanwaltskammern als Selbstverwaltungsaufgabe wahrgenommen werden.

Mit freundlichen Grüßen

Katja Meier