Deutscher Bundestag **Drucksache 19/19105**

19. Wahlperiode 12.05.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Roman Müller-Böhm, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/17930 –

Legal Tech bei Sicherheitsbehörden

Vorbemerkung der Fragesteller

Der Kriminalstatistik des Bundeskriminalamtes zufolge wurden im Jahr 2018 insgesamt 5,56 Millionen Straftaten erfasst (https://de.statista.com/statistik/daten/studie/197/umfrage/straftaten-in-deutschland-seit-1997/). Die Aufklärungsquote der Polizei lag bei etwa 58 Prozent (https://de.statista.com/statistik/daten/studie/2303/umfrage/entwicklung-der-aufklaerungsquote-von-straftaten-seit-1989/). Der Einsatz von Software gehört schon länger zu einem bewährten Werkzeug der Ordnungshüter. Die Einsatzmöglichkeiten sind dabei für viele Bereiche der Beamten denkbar. So setzt die hessische Polizei ein Programm zur Koordination ihrer Einsätze (https://www.crn.de/software-services/software-tuning-fuer-die-polizei.121298.html) und Nordrhein-Westfalen (NRW) in diesem Jahr eine neue Recherchesoftware ein (https://www.aachener-zeitung.de/nrw-region/nrw-polizei-fuehrt-neues-recherche-system-ein_aid-48300823). Darüber hinaus werden spezielle Programme zur Bekämpfung von Kinderpornografie eingesetzt, welche in Zusammenarbeit mit Forschung und Privatwirtschaft entwickelt wurden (https://www.im.nrw/themen/polizei/nrw-verstaerkt-kampf-gegen-kinderpornografie-und-missbrauch).

Auch bei der Bundespolizei findet Software Verwendung. Seit Mitte 2019 testet die Bundespolizei an Bahnhöfen gemeinsam mit der Deutschen Bahn eine intelligente Videoanalyse-Technik (https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2019/06/190607_videoanalyse.html) und das BKA verwendet ein besonderes System zur Gesichtserkennung (https://www.crn.de/software-services/polizei-verfuegt-ueber-5-8-millionen-fotos.121671.html).

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbe-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 11. Mai 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

dürftigkeit der erfragten Informationen der oben genannten Bundesbehörden eine Beantwortung sämtlicher Fragen im Rahmen dieser Kleinen Anfrage in offener Form ganz oder teilweise nicht erfolgen kann.

Im Einzelnen:

Die Antworten zu den Fragen 1 mit Unterfragen, 2 mit Unterfragen, 3 bis 7, 9 mit Unterfragen, 10 mit Unterfragen 11 mit Unterfragen sowie 12 bis 14 sind in Teilen als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Dienststellen des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb sind die Antworten zu den genannten Fragen gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (VS-Anweisung – VSA) in Teilen als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Soweit sich die Fragestellung auf die Nachrichtendienste des Bundes bezieht, ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass sämtliche Fragen mit Ausnahmen der Fragen 8 und 15 Fragen nicht beantwortet werden können. Gegenstand der Fragen sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt.

Eine Bekanntgabe von Einzelheiten zu der im Rahmen der Aufgabenerfüllung genutzten Software würde weitgehende Rückschlüsse auf die technischen Fähigkeiten und unmittelbar auf die technische Ausstattung und das Aufklärungspotential der Nachrichtendienste des Bundes zulassen. Dadurch könnten die Fähigkeiten der Nachrichtendienste des Bundes, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung der Nachrichtendienste des Bundes jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies betrifft insbesondere die Möglichkeiten zur Aufklärung nationaler und internationaler terroristischer Bestrebungen, bei denen derartige Kommunikationsmittel in besonderem Maße von den beobachteten Personen genutzt werden.

Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten der Nachrichtendienste des Bundes bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten der Nachrichtendienste des Bundes gewinnen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes (§ 1 Absatz 2

Gesetz über den Bundesnachrichtendienst, § 3 Absatz 1 Bundesverfassungsschutzgesetz, § 1 Absatz 1 und § 14 Absatz 1 Gesetz über den militärischen Abschirmdienst) nicht mehr sachgerecht erfüllt werden könnte.

Soweit die Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben Bundeskriminalamt (BKA), Bundespolizei (BPOL) und Zollkriminalamt / Financial Intelligence Unit (ZKA / FIU) von den Fragestellungen betroffen sind, kann die Beantwortung aller Fragen mit Ausnahme der Fragen 8, 9 und 15 ebenfalls nicht bzw. nicht vollumfänglich erfolgen.

Eine Bekanntgabe von Einzelheiten der bei diesen Behörden zur Bekämpfung von Kriminalität und Terrorismus im Rahmen ihrer jeweiligen Zuständigkeit eingesetzten Softwareprodukte für die Bearbeitung und Auswertung von Ermittlungsverfahren würde weitgehende Rückschlüsse auf die technischen Fähigkeiten sowie die taktischen Einzelheiten bzw. Arbeitsabläufe und damit mittelbar auch sowohl auf die derzeitige als auch die geplante technische Ausstattung sowie das Strafverfolgungs- und Gefahrenabwehrpotenzial dieser Behördenzulassen.

Diese taktischen Einzelheiten umfassen insbesondere die hier von den Fragestellungen umfassten Methoden zur forensischen Sicherung und Analyse, Umgehung oder Entsperrung von Verschlüsselungen sowie das Einbringen von Software, darüber hinaus auch die Informationen über den konkreten operativen Einsatz entsprechender Software inklusive der Frage über etwaige Alternativen. Durch ein Bekanntwerden der genannten Methoden könnten die Fähigkeiten der Sicherheitsbehörden mit polizeilichen Aufgaben, Erkenntnisse im Wege der technischen Strafaufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden, insbesondere, wenn keine ausreichenden Alternativen zu den für die Strafverfolgung und Gefahrenabwehr genutzten Produkten zur Verfügung stehen. Denn Beschuldigte könnten sich somit gezielt eben jener Strafverfolgung und Gefahrenabwehr entziehen, etwa durch Maßnahmen zur Hinderung des Einsatzes der entsprechenden Software. Dies ist jedoch nicht hinnehmbar, da die Gewinnung von Informationen durch eine IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr ist aber für die Aufgabenerfüllung dieser Behörden und damit für die Sicherheit der Bundesrepublik Deutschland und bei der Bekämpfung vor allem des Terrorismus, der Politisch motivierten sowie der Organisierten Kriminalität unerlässlich ist. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies würde folgenschwere Einschränkungen der Strafverfolgung und Gefahrenabwehr bedeuten, womit letztlich die gesetzlichen Aufträge von BKA – verankert im Grundgesetz (Art. 73 Nr. 10 GG, Art. 87 GG) und im Bundeskriminalamtgesetz (BKAG), BPOL (Art. 87 GG sowie Bundespolizeigesetz [BPolG]) und ZKA/FIU (Art. 87 GG, Zollfahndungsdienstgesetz [ZFdG], Geldwäschegesetz [GwG], Unionszollkodex [UZK]) – nicht mehr sachgerecht erfüllt werden könnten.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Informationen sowohl für die Aufgabenerfüllung der Nachrichtendienste des Bundes als auch der Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, mittels welcher technischen Produkte die Sicherheitsbehörden z. B. von der Telekommunikationsüberwachung Gebrauch machen, könnte zu einer Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, die eine weitere Aufklärung der von diesen verfolgten Be-

strebungen und Planungen unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

Es ist jedoch unklar, in welchen Bereichen die jeweilige Technik zum Einsatz kommt, welche Technik noch in der Testphase steckt und welche bereits zum festen Repertoire gehört. Es ist nach Ansicht der Fragesteller fraglich, inwiefern die Bundesregierung gemeinsam mit Forschung und Unternehmen Software zur Sichtung und zu einer ersten rechtlichen Bewertung entwickelt oder einen solchen Auftrag vergeben hat und ob dabei der Nutzen und die Wahrung der Bürgerrechte im Einklang stehen.

1. Welche Software wird von der Bundespolizei beziehungsweise vom Bundeskriminalamt oder von einer anderen Sicherheitsbehörde des Bundes zu präventiven Tätigkeiten verwendet?

   a) Welche Software wird dabei für welchen Fachbereich verwendet?

   b) Von welchem Hersteller wurde die jeweilige Software zur Verfügung gestellt?

   c) Falls eine Lizenz erworben wurde, wie lange laufen für die jeweilige Software die Lizenzen?

   d) In welcher Höhe werden dabei Steuermittel ausgegeben (bitte nach Jahr, Behörde, Verwendung und unter Angabe der Fundstelle im Haushaltsplan aufschlüsseln)?

Die Frage 1 und ihre Unterfragen werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Eine grundsätzliche Unterscheidung von Softwareprodukten in präventive und repressive Nutzung ist aus Sicht der Bundesregierung wenig sinnhaft, da unterschiedliche Funktionen und Features einer Software sowohl Komponenten für eine Nutzung in der Prävention oder auch der Repression enthalten können. Der Verwendungszweck von Softwareprodukten kann verschiedene Einsatzgebiete umfassen.

Software zur präventiven Tätigkeit bei den Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben umfasst sämtliche Software, welche als Führungs- und Einsatzmittel in der Kriminalitätsbekämpfung genutzt wird.

Auch Anwendungen zur inhaltlichen Datenträgerauswertung oder Hashwertdatenbanken zur Erkennung pornographischer Schriften oder auch Hinweisportale werden für präventive Zwecke, hauptsächlich jedoch zu repressiven Zwecken, genutzt. IT-Verfahren zur Risikoanalyse sowie zum Risikomanagement werden zu präventiven, Software zur Datenanalyse sowohl zu präventiven als auch repressiven Zwecken genutzt.

Darüber hinaus kommen auch die zentralen Systeme INPOL und INZOLL sowie das Schengener Informationssystem zum Einsatz.

Im Übrigen wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil verwiesen.

Weitere Ausführungen können mit Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

2. Welche Software wird von der Bundespolizei beziehungsweise vom Bundeskriminalamt oder von einer anderen Sicherheitsbehörde des Bundes zu repressiven Tätigkeiten verwendet?

   a) Welche Software wird dabei für welchen Fachbereich verwendet?

   b) Von welchem Hersteller wurde die jeweilige Software zur Verfügung gestellt?

   c) Falls eine Lizenz erworben wurde, wie lange laufen für die jeweilige Software die Lizenzen?

   d) In welcher Höhe werden dabei Steuermittel ausgegeben (bitte nach Jahr, Behörde, Verwendung und unter Angabe der Fundstelle im Haushaltsplan aufschlüsseln)?

Die Frage 2 und ihre Unterfragen werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Software zur repressiven Tätigkeit bei den Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben umfasst sämtliche Software, welche z. B. zur Vorgangsbearbeitung, zur Fallbearbeitung, Fahndungs- und Auskunftssystem, erkennungsdienstliche Verfahren genutzt wird. Ferner werden zur forensischen Sicherung, Analyse und zu Auswertezwecken ebenfalls unterschiedliche kommerzielle und eigens entwickelte Produkte genutzt, die entsprechend des Einzelfalles zur Anwendung kommen.

Im Übrigen wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil verwiesen.

Weitere Ausführungen können mit Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

3. Welche Software wird von der Bundespolizei beziehungsweise vom Bundeskriminalamt oder von einer anderen Sicherheitsbehörde des Bundes zu Recherche- und Analysezwecken verwendet?

4. Welche Software wird dabei für welchen Fachbereich verwendet?

5. Von welchem Hersteller wurde die jeweilige Software zur Verfügung gestellt?

6. Falls eine Lizenz erworben wurde, wie lange laufen für die jeweilige Software die Lizenzen?

7. In welcher Höhe werden dabei Steuermittel ausgegeben (bitte nach Jahr, Behörde, Verwendung und unter Angabe der Fundstelle im Haushaltsplan aufschlüsseln)?

Die Fragen 3 bis 7 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Bei den Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben kommen im Bereich der Recherche und Analyse Produkte beispielsweise zur inhaltlichen Datenträgerauswertung sowie zur Analyse von Daten bereits im System

INPOL-Fall implementierte Recherchefunktionen zum Einsatz sowie eigens in den Behörden entwickelte Produkte.

Die FIU nutzt für die operative und strategische Analyse die von den Vereinten Nationen bereitgestellte spezifische FIU-Software GoAML. Daneben wird die entsprechende IT-Plattform FIU.Net für den sicheren Datenaustausch der FIUs der Mitgliedstaaten genutzt.

Im Übrigen wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil verwiesen.

Weitere Ausführungen können mit Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

8. Auf welcher gesetzlichen Grundlage beruht der Einsatz der jeweiligen Software bei der Bundespolizei beziehungsweise beim Bundeskriminalamt oder bei einer anderen Sicherheitsbehörde des Bundes?

Der Einsatz entsprechender Software erfolgt auf Grundlage der durch allgemein geltenden Rechtsgrundlagen wie die StPO sowie auf durch spezialgesetzlich zugeeingeräumten Ermächtigungen.

9. Welche Software wurde bisher bei der Bundespolizei beziehungsweise beim Bundeskriminalamt oder bei einer anderen Sicherheitsbehörde des Bundes getestet und nach entsprechender Evaluation nicht weiter eingesetzt?

   a) Welche Software wurde dabei für welchen Fachbereich verwendet?

   b) Von welchem Hersteller wurde die jeweilige Software zur Verfügung gestellt?

   c) Falls eine Lizenz erworben wurde, wie lange laufen für die jeweilige Software die Lizenzen?

   d) In welcher Höhe wurden dabei Steuermittel ausgegeben (bitte nach Jahr, Behörde, Verwendung und unter Angabe der Fundstelle im Haushaltsplan aufschlüsseln)?

Die Frage 9 und ihre Unterfragen werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet:

Beim ZKA sowie der FIU kam es zu keinem entsprechenden Vorgang.

Beim BKA liegen keine retrograden Aufzeichnungen über ggf. getestete und nach entsprechender Evaluation nicht weiter eingesetzte Softwareprodukte vor.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

10. Welche Software wird künftig bei der Bundespolizei beziehungsweise beim Bundeskriminalamt oder bei einer anderen Sicherheitsbehörde des Bundes eingesetzt beziehungsweise getestet?

    a) Welche Software soll dabei für den jeweiligen Fachbereich verwendet werden?

Die Fragen 10 und 10a werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

BKA:

Das BKA wird im Rahmen des Pilotprojektes EPRIS (European Police Records Index System) gemeinsam mit anderen Mitgliedstaaten der Europäischen Union sowie Europol die sogenannte „ADEP-Technologie“ testen. Die Software wurde zur Optimierung des internationalen polizeilichen Informationsaustausches entwickelt.

Das BKA erprobt zurzeit eine Softwarelösung zur Bewertung der Qualität von Finger- und Handflächenabdrücken vor ihrer Verarbeitung im Automatisierten-Fingerabdruck-Identifizierungs-System (AFIS). Der Einsatz der Software soll der Erhöhung der Datenqualität der im Rahmen von erkennungsdienstlichen Behandlungen erhobenen Finger- und Handflächenabdrücke dienen und in Folge die Identifizierungsquote von Straftätern bzw. Tatverdächtigen erhöhen. Ihr Einsatz ist damit in erster Linie dem repressiven Bereich zuzuordnen. Die Softwarelösung wird noch nicht im Wirkbetrieb eingesetzt.

International findet im Bereich der Bekämpfung des sexuellen Missbrauchs von Kindern die sog. ICSE-Datenbank (International Child Sexual Exploitation database) Anwendung. Es handelt sich um eine Bildvergleichsdatenbank von Interpol, in die weltweit kinderpornografisches Material von Sicherheitsbehörden eingespeist wird. Europol ist ebenfalls angebunden, für Deutschland nimmt das BKA als Zentralstelle die Datenpflege war. Ziel ist es, – wie bei der nationalen Bildvergleichsdatenbank – neu eingehendes Missbrauchsmaterial mit der Datenbank abgleichen zu können, um feststellen zu können, ob dieses einem bereits geklärten Fall zugeordnet werden kann oder ob intensive Ermittlungsmaßnahmen zur Aufklärung des Missbrauchsfalls geboten sind.

FIU:

Die FIU testet mit dem Ziel des künftigen Einsatzes für die operative Analyse das Analyseprogramm FIU-Analytics.

Darüber hinaus wird künftig der Einsatz der Softwareanwendung IDEA (Interactive Data Extraction and Analysis) im Bereich der strategischen Analyse erfolgen.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Weitere Angaben können unter Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

b) Von welchem Hersteller wird die jeweilige Software zur Verfügung gestellt?

BKA:

Bei der bei der Antwort zu Frage 10a genannten „ADEP-Technologie“ handelt es sich um eine eigens vom Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS) entwickelte Software.

Bei der ebenfalls genannten Softwarelösung zur Bewertung der Qualität von Finger- und Handflächenabdrücken vor ihrer Verarbeitung im Automatisierten-Fingerabdruck-Identifizierungs-System (AFIS) handelt es sich um eine Eigenentwicklung des BKA auf der Basis von Open-Source Produkten.

Darüber hinaus wird auf die Antwort zu Frage 10a verwiesen.

FIU:

Bei der Software FIU-Analytics handelt es sich um eine Eigenentwicklung des Zolls. Die Software IDEA wird von der Audicon GmbH zur Verfügung gestellt.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

c) In welcher Höhe sollen dabei Steuermittel ausgegeben werden (bitte nach Jahr, Behörde, Verwendung und unter Angabe der Fundstelle im Haushaltsplan aufschlüsseln)?

BKA:

Das europäische Projekt zur Erprobung der „ADEP-Technologie“ wird in den Haushaltjahren 2020 und 2021 durch die Europäische Kommission mit rund einer Million Euro gefördert. Darüber hinaus erfolgt eine finanzielle Beteiligung des Programms Polizei 2020 im Haushaltsjahr 2020 in Höhe von rund 840.000 Euro (Kapitel 0612 Titel 532 02, Kapitel 0624 Titel 532 01).

Für das Projekt zur Erprobung einer Softwarelösung für das System AFIS wurden bisher insgesamt ca. 10.000 Euro verausgabt, vorrangig für Hardwarekomponenten, die im Kontext der Komplementierung auch für weitere Projekte genutzt werden können.

FIU:

FIU-Analytics:

2018: 424.700,97 Euro

2019 (bis September): 825.992,91 Euro

2020: ca. 1,5 Millionen Euro

IDEA:

2020: 1.920,00 Euro

2021: 960,00 Euro

2022: 960,00 Euro

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

11. Entwickelt die Bundesregierung gemeinsam mit Forschung und Unternehmen Software zum Einsatz bei Sicherheitsbehörden, beispielsweise zur Datensichtung und zu einer ersten rechtlichen Bewertung zur Bekämpfung von Kinderpornografie, oder hat sie einen entsprechenden Auftrag vergeben?

    a) Wenn ja, mit welchen Unternehmen beziehungsweise welchen Forschungseinrichtungen wird zusammengearbeitet?

Die Fragen 11 und 11a werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die FIU entwickelt derzeit in Zusammenarbeit mit einem IT-Dienstleistungsunternehmen die Software namens FIU-Analytics.

Das ZKA ist an keiner der in Rede stehenden Software-Entwicklungen beteiligt.

Das BKA entwickelt in Kooperation mit dem Fraunhofer Institut eine auf künstlicher Intelligenz basierende Software, die in der Lage sein soll, kinderpornografisches Material aus einem Datenbestand herausfiltern zu können.

Des Weiteren betreibt das BKA als Zentralstelle Kinderpornografie die von einer externen Firma entwickelte Hashdatenbank Pornografische Schriften (HashDB PS).

Das BKA nutzt zudem eine von einer externen Firma entwickelte Bildvergleichsdatenbank, in der Bild- und Videomaterial zu identifizierten und nicht identifizierten Opfern und Tätern des sexuellen Missbrauchs für ganz Deutschland zentral eingestellt wird.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen. Weitere Angaben können unter Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

    b) Wenn ja, zu welchen Zwecken wird Software entwickelt, und welche Ziele werden verfolgt?

FIU:

Die Software FIU-Analytics soll im Bereich der operativen Analyse zur risikobasierten Vorbewertung eingehender Verdachtsmeldungen und sonstiger Informationen eingesetzt werden.

BKA:

Das BKA entwickelt in Kooperation mit dem Fraunhofer Institut eine auf künstlicher Intelligenz basierende Software, die in der Lage sein soll, kinderpornografisches Material aus einem Datenbestand herausfiltern zu können. Die BKA-Forschungsstelle Cybercrime führt dazu aktuell eine eigene Machbarkeitsstudie („TRAFFIIC“) durch. Dadurch könnte Beweismaterial, welches bei Durchsuchungen sichergestellt wurde, effizienter ausgewertet werden. Dies betrifft insb. die Polizeidienststellen der Bundesländer.

Das BKA betreibt als Zentralstelle Kinderpornografie die von einer externen Firma entwickelte Hashdatenbank Pornografische Schriften (HashDB PS). Die Datenbank wird im BKA im einem eigens entwickelten Workflow zur automatisierten Vorbewertung von strafrechtlich relevanten Dateien verwendet. Diese werden dabei auf Hashwertgleichheit oder Photo-DNA-Ähnlichkeit überprüft und automatisiert bewertet. Dies ermöglicht es, die täglich beim BKA einge-

henden Hinweise auf den Besitz und die Verbreitung von Kinderpornografie effizient zu bearbeiten (Quantität) und ein hohes Niveau (Qualität) zu erreichen.

Das BKA nutzt zudem eine von einer externen Firma entwickelte Bildvergleichsdatenbank, in der Bild- und Videomaterial zu identifizierten und nicht identifizierten Opfern und Tätern des sexuellen Missbrauchs für ganz Deutschland zentral eingestellt wird. Die Datenbank dient dazu, neu eingehende Dateien bereits bekannten Serien des sexuellen Missbrauchs von Kindern zuordnen zu können, um so Doppelarbeit und eine Reviktimisierung zur vermeiden.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

12. Welche Projekte verfolgt die Bundesregierung gemeinsam mit anderen Bundesländern hinsichtlich des Einsatzes von Software bei Sicherheitsbehörden, beispielsweise zur Datensichtung und zu einer ersten rechtlichen Bewertung zur Bekämpfung von Kinderpornografie?

Das ZKA und die FIU verfolgen keine solchen Projekte.

BKA:

Die Hashdatenbank für kinderpornografische Schriften (HashDB PS) ist eine Sammlung von Hashwerten bekannter kinder- und jugendpornografischer Dateien, die das Bundeskriminalamt den Bundesländern für Abgleichzwecke zur Verfügung stellt. Wird ein Datenträger im Bundesland sichergestellt, so kann dieser mit der Sammlung abgeglichen werden und gibt erste Hinweise auf den Inhalt des Datenträgers. Dies ermöglicht eine schnellere und effizientere Auswertung des sichergestellten Beweismaterials.

Hierbei werden fortlaufend andere technische Lösungen geprüft und bei erkannter Praxisreife in den Workflow implementiert.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen. Weitere Angaben können unter Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

13. Welche Projekte verfolgt die Bundesregierung gemeinsam mit anderen Mitgliedstaaten der Europäischen Union hinsichtlich des Einsatzes von Software bei Sicherheitsbehörden, beispielsweise zur Datensichtung und zu einer ersten rechtlichen Bewertung zur Bekämpfung von Kinderpornografie?

BKA:

Das BKA ist im Austausch mit anderen EU-Mitgliedstaaten über vorliegende Erfahrungen im Zusammenhang mit technischen Lösungen bei der Bekämpfung der Kinderpornografie. Eine gemeinsame Befassung innerhalb eines konkreten Projekts erfolgt derzeit nicht.

ZKA:

Im Bereich der Sicherheitsrisikoanalyse der EU-Zollverwaltungen arbeiten die Mitgliedstaaten gemeinsam mit der EU-Kommission sowie Norwegen und der Schweiz an einer Verbesserung des bestehenden EU-Risikoanalysesystems ICS (Import Control System) zum sogenannten „ICS2“.

ICS 2 soll vor allem die Echtzeitkommunikation der beteiligten Mitgliedstaaten bei der Risikoanalyse verbessern und die Zusammenarbeit fördern.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Weitere Angaben können unter Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

14. Welche Projekte verfolgt die Bundesregierung gemeinsam mit Einrichtungen und Behörden der Europäischen Union, beispielsweise Europol, hinsichtlich des Einsatzes von Software bei Sicherheitsbehörden, beispielsweise zur Datensichtung und zu einer ersten rechtlichen Bewertung zur Bekämpfung von Kinderpornografie?

BKA:

Hinsichtlich des BKA wird auf die Antwort zu Frage 10a verwiesen.

ZKA:

Im Rahmen des unter Frage 13 beschriebenen Projektes ist auch die Einbindung von Europol- und EU-Kommissions-Systemen (hier insbesondere das Europol Information System [EIS] und das Schengen Information System [SIS]) in ICS 2 angedacht.

Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Weitere Angaben können unter Verweis auf die Vorbemerkung nicht gemacht werden.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

15. Wie wird die Qualität der eingesetzten Software und Algorithmen gewährleistet?

a) Gibt es Standards oder Verfahren, um die Qualität zu sichern?

Wenn ja, welche?

b) Findet eine Rückkoppelung während des Betriebs statt, um beispielsweise herauszubekommen, ob ein Algorithmus auf einer fehlerhaften Datenbasis geschult wurde oder falsche Kriterien verwendet wurden?

c) Wer ist für die Sicherung der Qualität der eingesetzten Software und Algorithmen zuständig?

Die Frage 15 und ihre Unterfragen werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Der Einsatz von Software bei den Sicherheitsbehörden erfolgt im Rahmen ihrer gesetzlichen Vorgaben. Die datenschutzrechtliche Konformität wird regelmäßig durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit überprüft.

Die tatsächlich produktbezogene Qualität der bei den Sicherheitsbehörden eingesetzten Softwareprodukte wird durch begleitende Qualitätssicherungsmaßnahmen sichergestellt, die bereits im Planungsstadium ansetzen. Dabei ist das

Testen der Software, etwa im Hinblick auf die technische Umsetzung und ihre Verträglichkeit mit vorhandenen Systemen sowie die Erfüllung der Forderungen des Bedarfsträgers, wesentlich. Eine Anpassung der sich in der Nutzung befindenden Software erfolgt mittels Softwarepflege/-änderungsmaßnahmen, die sowohl durch den nutzenden Fachbereich als auch durch den technischen Betrieb initiiert werden können.

Die Sicherung der Qualität der eingesetzten Software (und dieser zu Grunde liegender Algorithmen) erfolgt zum einen durch die jeweiligen Hersteller, die auf Basis entsprechender Softwarepflege- bzw. Wartungsverträge Patches und Updates bereitstellen. Darüber hinaus erfolgt durch die Behörden selbst eine regelmäßige und fortlaufende Qualitätskontrolle, beispielsweise durch den Abgleich von vordefinierten Standardtestszenarien und die Überprüfung erzielter Ergebnisse.

Ein weiterer Bestandteil der Qualitätssicherung ist die Sicherstellung eines sach- und fachgerechten Einsatzes der Softwareprodukte durch die Anwender. Zu diesem Zweck werden seitens der Sicherheitsbehörden umfangreiche Schulungsmaßnahmen durchgeführt, die im Falle von sehr speziellen Softwareprodukten bis hin zu Schulungen von Einzelanwendern gewährleistet werden.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333