BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

An den Stellvertretenden Vorsitzenden des
Ausschusses für Inneres und Heimat
Herrn Prof. Dr. Lars Castellucci

per E-Mail: innenausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat32@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 16.04.2024
GESCHÄFTSZ. 32-642-1/028#0065

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Einladung zur öffentlichen Anhörung im Innenausschuss am 22. April 2024**
BEZUG Antrag der Fraktion der CDU/CSU "Handlungsfähigkeit der Strafverfolgungsbehörden sichern - Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren" BT-Drs. 20/9495
ANLAGEN Stellungnahme

Sehr geehrter Herr Professor Dr. Castellucci,

zunächst bedanke ich mich für die Einladung zur öffentlichen Anhörung im Innenausschuss am 22. April 2024. Die Teilnahme wurde bereits zugesagt.

Anbei übersende ich meine schriftliche Stellungnahme mit der Bitte um Weiterleitung an die Mitglieder des Ausschusses.

Mit freundlichen Grüßen

Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 16.04.2024

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags
am 22. April 2024

Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren

(BT-Drs. 20/9495)

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Ausgangslage

Mit dem Gesamtprogramm Polizei 20/20 (P 20) haben sich die Innenminister des Bundes und der Länder 2016 darauf geeinigt, die polizeiliche IT-Landschaft grundlegend zu modernisieren. Kern von P 20 ist das „gemeinsame Datenhaus“ der Polizeibehörden des Bundes und der Länder. Das Datenhaus soll durch eine mandantenfähige Trennung sicherstellen, dass jeder Teilnehmer – also jede Polizeibehörde – personenbezogene Daten entsprechend seiner jeweiligen rechtlichen Grundlagen speichert bzw. verarbeitet und dabei gesetzliche Speicherschwellen und den Grundsatz der Zweckbindung einhält.

Ein weiteres Ziel von P 20 ist es, den Datenbestand – innerhalb der gesetzlichen und verfassungsrechtlichen Grenzen – von vornherein auswertbar und analysefähig auszurichten. Deshalb werden alle Daten im gemeinsamen Datenhaus gespeichert, nicht mehr in vielen unterschiedlichen Systemen. Zu diesem Zwecke wird es innerhalb von P 20 eine Domäne „Analyse und Auswertung“ geben.

Die derzeit betriebenen Systeme werden teilweise als Interimssysteme in das Projekt P20 überführt, um eine Zwischenlösung bereitstellen zu können, bis das Datenhaus fertiggestellt ist. Dies betrifft etwa verschiedene Vorgangsbearbeitungssysteme und Fallbearbeitungssysteme. Natürlich wird auch das bisherige INPOL-Zentral übergangsweise weiterbetrieben. Um in dieser Zeit auch innerhalb der Domäne „Analyse und Auswertung“ weitergehende Möglichkeiten zu haben, nutzen bereits einige Teilnehmer einzelne Werkzeuge und Tools, die jeweils Teile der geplanten Domäne „Analyse und Auswertung“ abdecken.[1] Als Beispiel: die hessische Polizei nutzt ein Softwareprodukt der Firma Palantir mit der Bezeichnung hessenData. Unter dem Namen DAR nutzt die Polizei in Nordrhein-Westfalen ebenfalls ein solches Produkt.

Das Bayerische Landeskriminalamt führte im Jahr 2022 eine europaweite Ausschreibung für ein Auswerte- und Analysesystem durch. Das Ausschreibeverfahren zu einer verfahrensübergreifenden Auswertung und Analyse wurde zugunsten einer Software der Firma Palantir Technologies GmbH entschieden. Dieses Analysetool wird in Bayern als verfahrensübergreifendes Recherche- und Analysesystem kurz „VeRA“ bezeichnet. VeRA ist daher der gebräuchliche Begriff für die Softwareprodukte „Foundry“ und „Gotham“ der Firma Palantir.

Durch Abschluss eines Rahmenvertrages eröffnete die bayerische Polizeibehörde anderen Polizeibehörden des Bundes und der Länder die Möglichkeit, ohne ein gesondertes Ausschreibeverfahren

[1] Fachlicher Bebauungsplan des Programms P 20 S. 65

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

ebenfalls das Softwareprodukt der Firma Palantir zu nutzen. Insoweit wird von einer sog. „Bundes-VeRA“ gesprochen.

Das Bundesministerium des Innern und für Heimat (BMI) hatte zunächst Interesse an VeRA bekundet, sich letztlich aber gegen das Produkt entschieden.

2. Funktionalitäten von VeRA

VeRA eröffnet umfangreiche Analysemöglichkeiten.

Ziel von VeRA bzw. ähnlichen Produkten der Firma Palantir ist es, umfangreiche und zu verschiedenen Zwecken betriebene polizeiliche Datenbestände zusammenzuführen, zu verknüpfen und auszuwerten. Je nach Bedarf des jeweiligen Nutzers können unterschiedliche Datenbanken und Systeme angebunden werden.

Neben polizeilichen Datenbanken wie Vorgangsbearbeitungssystemen und polizeilichen Informationssystemen (z.B. INPOL-Zentral) können auch externe Datenbanken in eine Analyse einbezogen werden. Hier kommen als Beispiele Datenbanken des Einwohnermeldeamtes und des Kraftfahrtbundesamtes in Betracht.

Polizeiliche Datenbanken enthalten nicht nur Speicherungen über Personen, die Gegenstand polizeilicher Ermittlungen sind, bzw. waren, sondern auch personenbezogene Daten von Betroffenen, die zu keinem Zeitpunkt einem strafrechtlichen Anfangsverdacht ausgesetzt waren. Unbeteiligte Dritte wie z. B. Opfer, Hinweisgeber, Zeugen und Anzeigenerstatter werden ebenfalls in polizeilichen Datenbanken gespeichert. Diese Daten können unter Umständen sehr sensibel sein, man denke nur beispielsweise an elektronische Vernehmungsprotokolle der Opfer von Sexualstraftaten.

3. Rechtfertigung von Auswerte- und Analyseverfahren

Auswerte- und Analyseverfahren sind nicht grundsätzlich unzulässig, bedürfen aber spezifischer Grundlagen. Diese liegen derzeit weder für das BKA noch für die Bundespolizei vor.

Das BVerfG hat in seiner Entscheidung vom 16.02.2023[2] ausgeführt, dass eine automatisierte Datenauswertung und Analyse nicht grundsätzlich unzulässig ist. Es hat aber klargestellt, dass sie ein

[2] 1 BvR 1547/19, 1 BvR 2634/20

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

eigenständiger Grundrechtseingriff sein kann, der deshalb auch einer eigenständigen Rechtsgrundlage bedarf. Der Gesetzgeber muss die Voraussetzungen und Bedingungen der Datenanalyse normenklar bestimmen. Umso schwerer die von der Datenanalyse ausgehenden Grundrechtseingriffe sind, desto höhere Schwellen muss der Gesetzgeber festlegen.

Gegenstand des Verfahrens waren seinerzeit landesgesetzliche Normen, auf dessen Grundlage die Polizei Hessen unter dem Namen hessenDATA Software der Firma Palantir einsetzte. Ebenfalls waren gesetzliche Regelungen Gegenstand des Verfahrens, die der Polizei Hamburg den Einsatz einer entsprechenden Software ermöglichen könnte. Diese bestimmten jedoch keine ausreichenden Schwellen und Grenzen.

In seinem Urteil hat das Bundesverfassungsgericht zum einen umfangreiche Kriterien aufgestellt, durch welche die Eingriffsintensität von Datenauswertungen und Analysen bestimmt werden kann. Zum anderen hat es Vorgaben aufstellt, durch welche ein Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt sein kann.

Die besondere Eingriffsintensität von automatisierten Auswerte- und Analysemöglichkeiten wird schon dadurch verdeutlicht, dass das Bundesverfassungsgericht einen Grundrechtseingriff in zweifacher Hinsicht angenommen hat. Zum einen stelle die Nutzung der Daten über den ursprünglichen Zweck hinaus einen Grundrechtseingriff dar. Zum anderen liege ein weiterer Eingriff in der automatisierten Datenanalyse selbst.

Für die Bestimmung des Eingriffsgewichts hebt das BVerfG zwei Kriterien besonders hervor. Das sind *„Art und Umfang der Daten“* sowie die *„Analysemethoden“.*

Um die besondere Tragweite für den Bereich der Bundespolizeibehörden verstehen zu können, muss man wissen, dass die Polizeien umfangreiche Daten zu unterschiedlichen Personen in vielen Dateien speichern. Die Speicherung erfolgt zu unterschiedlichen Zwecken und derzeit noch in verschiedenen Dateisystemen.

In den Vorgangsbearbeitungssystemen - als Kernsysteme der Polizeien - werden beispielsweise neben Daten von Beschuldigten auch sensible Informationen von Opfern, von Zeugen und von Hinweisgebern zu unterschiedlichen Zwecken gespeichert. Es handelt sich also auch um einen umfangreichen Datenbestand von unbescholtenen Bürgerinnen und Bürgern. Diese personenbezogenen Daten würden potentiell mit VeRA ausgewertet und dann ggf. länger gespeichert werden. Vor diesem Hintergrund ist es offensichtlich, dass derart intensive Grundrechtseingriffe nicht auf Generalklauseln gestützt werden können. Daneben darf nicht vergessen werden, dass auch bei Daten

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

von Beschuldigten und Verdächtigten sich bei weitem nicht jeder Verdacht bestätigt. Viele Personen sind weiter gespeichert, auch wenn das Verfahren eingestellt oder sie freigesprochen wurden.

Es bleibt festzuhalten, dass das BVerfG mit seinem Urteil vom 16.02.2023 einen umfangreichen „Werkzeugkasten“ zur Verfügung gestellt hat, dessen Inhalt für eine spezialgesetzliche Grundlage genutzt werden muss.

4. Datenschutzrechtliche Herausforderungen

a. Bedarf einer Analysesoftware:

Zunächst obliegt es nicht dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, polizeifachliche Bedarfe zu erkennen und zu benennen.

Unabhängig davon bestehen aktuell bereits Auswerte- und Analysemöglichkeiten, die sowohl das BKA als auch die Bundespolizei unterstützen, Tat-Tat und Tat-Täter-Beziehungen in allen Phänomenbereichen zu erkennen. Hierzu werden die einheitlichen Fallbearbeitungssysteme genutzt (sog. eFBS).

b. Spezialgesetzliche Grundlage:

Wird ein darüberhinausgehender Bedarf für eine komplexere Auswertung und Analyse festgestellt, ist zunächst zu eruieren, ob eine gesetzliche Grundlage einen solchen Einsatz und damit Eingriff in das Recht auf informationelle Selbstbestimmungsrecht überhaupt rechtfertigen würde.

Eine den Vorgaben des Urteils des BVerfG vom 16.02.2023 entsprechende spezialgesetzliche Regelung der Polizeibehörden des Bundes (Bundeskriminalamt und Bundespolizei) liegt derzeit weder für VeRA noch für vergleichbare Produkte vor. Der Gesetzgeber hat vor dem Einsatz von Auswerte- und Analysesystemen eine entsprechende gesetzliche Grundlage zu schaffen. Anderenfalls würde das „Pferd von hinten aufgezäumt werden“ und eine Datenverarbeitung verstieße bereits gegen den Gesetzesvorbehalt.

Innerhalb des Gesetzgebungsverfahrens müssen u.a. entsprechend der Vorgaben des Bundesverfassungsgerichts folgende Fragen zuvor geklärt werden, bevor ein Auswerte- und Analysesystem in den Wirkbetrieb geht:

- Welche Datenbanken werden einbezogen?
- Werden nur Daten analysiert, die die jeweilige Behörde selbst erhoben hat?

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

- Werden polizeiliche Daten übergreifend ausgewertet, die mit unterschiedlichen Zielsetzungen gespeichert werden (z.B. entweder nur Daten von Personen, die zur Verfolgungsvorsorge im INPOL gespeichert sind oder aber auch Zeugendaten aus den Vorgangsbearbeitungssystemen?)
- Werden externe Datenbanken einbezogen?
- Werden Daten aus sozialen Netzwerken einbezogen?
- Werden Daten von Nachrichtendiensten einbezogen?
- Werden Daten von ausländischen Behörden berücksichtigt?
- Werden Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen einbezogen?
- Werden Daten automatisiert oder manuell einbezogen?
- Wer hat Zugriff auf das Analysetool?
- Wie komplex ist der dahinterstehende Algorithmus und wie ist es um die Nachvollziehbarkeit der Datenanalyse bestellt?

Aus diesen Antworten ergeben sich die Anforderungen an eine spezialgesetzliche Grundlage.

c. Polizeiliche Generalklauseln

Auf allgemeine polizeiliche Generalklauseln (z. B. § 16 Abs. 1 und Abs. 4 BKAG) lässt sich eine derartige Analysemöglichkeit jedenfalls nicht stützen. Schon die spezielleren Vorschriften aus dem hessischen bzw. hamburgischen Polizeirecht waren zu allgemein gehalten. Als praktisches Beispiel wird auf den Beratungs- und Kontrolltermin zu sog. Funkzellendatenbanken im BKA verwiesen.[3]

In dieser Funkzellendatenbank speichert das BKA personenbezogene Daten, die die Strafverfolgungsbehörden im Bund und Ländern durch Funkzellenabfragen – zu Rufnummern, IMEI, IMSI, LAC-Cell-ID, Datum, Uhrzeit, Gesprächsdauer, Gesprächsrichtung – erhoben haben. Das BMI stützt die Speicherung auf die Generalklausel des § 16 Abs. BKAG und den Abgleich auf § 16 Abs. 4 BKAG. Das Eingriffsgewicht kommt einer Rasterfahndung gleich und kann nicht auf Generalklausel gestützt werden. Ich habe die Einstellung dieser Dateien angeordnet. Ein Klageverfahren hiergegen ist derzeit vor dem Verwaltungsgericht Köln anhängig.

Produkte der Firma Palantir, bzw. VeRA könnten im Verhältnis zur Funkzellendatenbank noch deutliche größere Datenmengen intensiver auswerten und analysieren. Mit VeRA könnte sog. „Data-Mining“ betrieben werden. Dieses umfasst nach der Definition der Bundesregierung Verfah-

[3] 30. Tätigkeitsbericht des BfDI, Nr. 8.2.4

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

ren und Methoden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbstständig auf Zusammenhänge analysiert werde, um auf diesem Wege „neues Wissen“ zu generieren“.[4]

Es bedarf daher unbedingt spezialgesetzlicher Regelungen, um eine Auswertung und Analyse rechtskonform umzusetzen.

d. Zweckbindungsgrundsatz:

Aus datenschutzrechtlicher Betrachtung ist es zudem erforderlich zu klären, welche Vorkehrungen zur Sicherung des Grundsatzes der Zweckbindung getroffen werden. Der Zweckbindungsgrundsatz ist ein Grundpfeiler des deutschen und europäischen Datenschutzrechts.[5] Er dient insbesondere dazu, die Verhältnismäßigkeit staatlichen Handelns sicherzustellen und Bürger vor ungerechtfertigten Grundrechtseingriffen zu schützen.

Mit P 20 sollen künftig alle Daten der Polizeibehörden in einem gemeinsamen Datenhaus gespeichert werden. Das Datenhaus wäre faktisch die Grundlage für Auswerte und Analysemöglichkeiten. Durch die einheitliche Datenbasis im Datenhaus bestünde grundsätzlich die Möglichkeit, dass sämtliche Daten miteinander abgeglichen, kombiniert und verknüpft werden. Gerade vor diesem Hintergrund ist es essentiell, sicherzustellen, dass der Grundsatz der Zweckbindung eingehalten wird. Selbstverständlich sind die oben genannten rechtlichen und verfassungsrechtlichen Vorgaben innerhalb des neuen Datenhauses zu beachten.

e. Unterlaufen von gesetzlichen Schwellen

Durch komplexe Auswerte- und Analyseverfahren könnten gesetzliche Schwellen unterlaufen werden. In dem polizeilichen Informationsverbund INPOL-Z werden personenbezogene Daten zur Fahndung und zur Vorsorge gespeichert. Hierfür bestehen bestimmte gesetzliche Schwellen in §§ 18, 19, 29, 31 Bundeskriminalamtsgesetz (BKAG). Zum einen ist die sog. Verbundrelevanz – länderübergreifende, internationale oder erhebliche Bedeutung – bei einer Speicherung zu beachten. Eine weitere Schwelle ist die sog. Negativprognose. Eine Speicherung zur Vorsorgezwecken ist daher nur dann rechtmäßig, wenn zuvor geprüft wurde, ob eine weitere Speicherung wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstige Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind.

[4] BT-Drs. 17/11582, S. 3
[5] https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2021/07_Positionspapier-Zweckbindung-Polizei.html

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Diese gesetzlichen Schwellen dürfen durch Auswerte- und Analysemöglichkeiten nicht unterlaufen werden.

5. Digitale Souveränität

In den Datenbanken der Polizeibehörden des Bundes und der Länder werden umfangreiche Daten von unterschiedlichsten Personenkreisen gespeichert. Von „einfachen“ Daten bis hin zu besonders sensiblen Daten werden Daten von Verdächtigen, Beschuldigten und verurteilten Straftätern und teilweise von unbescholtenen Bürgern gespeichert. Vor diesem Hintergrund und mit Blick auf mögliche Gefahren für die Sicherung dieser sensiblen Daten ist die digitale Souveränität der Bundesbehörden ein verfassungsrechtliches Gebot. Das Bundesverfassungsgericht weist zutreffend darauf hin, dass beim Einsatz von Software privater Akteure oder anderer Staaten die Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte besteht.[6]

Aus datenschutzrechtlicher Sicht ist es daher zu begrüßen, wenn das Programm P 20 eine eigene Softwarelösung entwickelt. Der Schutz der Grundrechte der betroffenen Personen ist Aufgabe des Staates und kann durch eigene digitale Lösungen am besten sichergestellt werden. Anderenfalls besteht das Risiko, Abhängigkeiten mit privaten Anbietern einzugehen, die nicht immer vorhersehbar sein können. Unbemerkte Manipulation und Zugriffe sind nicht auszuschließen. Um eine verfassungsrechtlich nicht hinnehmbare Abhängigkeit der Polizeibehörden zu vermeiden, sind Eigenentwicklungen grundsätzlich vorzugszugswürdig.[7]

[6] 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[7] Kelber/Bortnikov, Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten, NJW 2023, 2002)

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de