

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Gollaleh Ahmadi (GRÜNE)

vom 4. März 2024 (Eingang beim Abgeordnetenhaus am 5. März 2024)

zum Thema:

Nachfrage zu Anfrage 19/17787 Palantir

und **Antwort** vom 21. März 2024 (Eingang beim Abgeordnetenhaus am 25. März 2024)

Senatsverwaltung für Inneres und Sport

Frau Abgeordnete Gollaleh Ahmadi (GRÜNE)

über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/18470
vom 04. März 2024
über Nachfrage zu Anfrage 19/17787 Palantir

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Wie positioniert sich der Senat zu der Einschätzung des Wissenschaftlichen Dienstes des Bundestages, der den Betrieb von Palantir für rechtswidrig hält? Welche Auswirkungen könnte diese Einschätzung auf die Entscheidung über den Einsatz von Palantir in Berlin haben?
2. Sofern der Senat an der Einführung von Palantir festhalten möchte, wie begründet er dies vor dem Hintergrund, dass inzwischen in mehreren Bundesländern Verfassungsbeschwerden gegen Nutzung und Testbetrieb laufen?
3. Begründet wird die Prüfung des Einsatzes der umstrittenen Software Palantir mit dem Umstand, dass diese "einen automatisierten Erkenntnisgewinn aus verschiedenen Quellen des vorhandenen polizeilichen Datenbestandes" ermögliche. Wie ist dies nach Auffassung des Senats vor dem Hintergrund zu rechtfertigen, dass auch die Polizei dem datenschutzrechtlich verankerten Zweckbindungsgrundsatz von Daten unterliegt?

Zu 1. bis 3.:

Das Bundesverfassungsgericht hat in seinem Urteil zu den polizeigesetzlichen Regelungen der Länder Hessen und Hamburg vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 - den Einsatz einer Software zur automatischen Verknüpfung und Auswertung von polizeilichen Datenbanken, wie sie von der Firma Palantir angeboten wird, für verfassungsrechtlich grundsätzlich zulässig erachtet, allerdings Vorgaben für eine verfassungskonforme Ausgestaltung der hierfür erforderlichen Rechtsgrundlagen gemacht, wie dies das Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages zur „Analyse polizeilicher Datenbanken - Verfassungsrechtliche Anforderungen an eine Rechtsgrundlage“ (WD 3 - 3000 - 145/23) vom 17. Januar 2024 auch zutreffend darstellt. Die Vereinbarkeit mit den vom Bundesverfassungsgericht in seiner Rechtsprechung entwickelten Grundsätzen der Zweckbindung und der Zweckänderung bei der Datenverarbeitung mit Hilfe der Software ist dabei eine der verfassungsrechtlichen Kernanforderungen an eine gesetzliche Regelung. Der Einsatz einer solchen Software im Land Berlin käme somit nur auf der Grundlage einer nach den Vorgaben des Bundesverfassungsgerichts ausgestalteten Rechtsgrundlage im Berliner Polizeirecht in Betracht.

4. Worüber konkret haben sich die Vertreter*innen der Bundesländer bei der IMK im Dezember 2023 ausgetauscht, über welche Aspekte bestand Konsens oder Dissens und welche Ergebnisse ließen sich ableiten? Inwiefern hatte dieser Austausch Auswirkungen auf Entscheidungen und Verfahrensweisen im Umgang mit Palantir?

Zu 4.:

Wie im Rahmen derartiger Gesprächsformate in Fachministerkonferenzen üblich, erfolgte die Erörterung mit dem Ziel der freien und offenen Meinungsbildung sowie ohne Protokollierung der Gesprächsverläufe.

5. Wie wurden Daten und Informationen bisher zusammengeführt und ausgewertet und wie geschieht dies in anderen Bundesländern, die nicht Palantir nutzen?

Zu 5.:

Sowohl der Abruf, als auch die Zusammenführung und Auswertung von polizeilichen Daten erfolgt innerhalb der Polizei Berlin manuell in mehreren, aufeinanderfolgenden Schritten und in den verschiedenen Dateisystemen. Der Prozess ist sehr aufwandsintensiv, und die Erkenntnisse liegen regelmäßig erst nach mehreren Stunden oder Tagen vor.

Nach hiesigem Kenntnisstand sind die Erfahrungswerte anderer Landes- und Bundesbehörden analog zu denen der Polizei Berlin.

6. Inwiefern gibt es alternative Anwendungen zu Palantir, um polizeiliche Datenbestände und Informationen „sachgerecht zusammenführen und so den aktuellen sicherheitsrelevanten Herausforderungen begegnen und Gefahren für höchste Rechtsgüter, insbesondere Leib und Leben von Personen, abwehren zu können“? (vgl. S19/17787) Welche Alternativen wären das, inwiefern unterscheiden sie sich von Palantir und welche Kosten würden dadurch entstehen, auch im Vergleich zu Palantir?

Zu 6.:

Nach Einschätzung des gemeinsamen Programms Polizei 20/20 des Bundes und der Länder ist es bislang keinem Hersteller im deutschen oder europäischen Raum möglich, die fachlichen und datenschutzrechtlichen Anforderungen in vergleichbarer Weise umzusetzen, wie sie von der Software von Palantir bereits erfüllt werden. Insbesondere die in dem zu 1. bis 3. bereits erwähnten Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 geforderten Kennzeichnungen von Daten sowie die Vorgaben zur hypothetischen Datenneuerhebung sind bislang nur durch die Nutzung der Software von Palantir realisierbar. Alternativprodukte gleicher fachlicher Qualität sind aktuell und auf absehbare Zeit nicht verfügbar. Das Produkt von Palantir deckt zudem durch jahrelange Entwicklungs- und Abstimmungsprozesse mit Hessen und Nordrhein-Westfalen die fachlichen und rechtlichen Anforderungen von deutschen Sicherheitsbehörden in Gänze ab.

7. Welche anderen Anwendungen wurden im Rahmen der EU-Ausschreibung, bei der Palantir schließlich den Zuschlag erhielt, in Betracht gezogen?

Zu 7.:

Die EU-Ausschreibung wurde durch den Freistaat Bayern initiiert und durchgeführt.

Es erfolgte die Durchführung eines transparenten Markterkundungsverfahrens und die Erstellung einer Leistungsbeschreibung. Im Anschluss veröffentlichte das Bayerische Landeskriminalamt die Ausschreibung am 18. Januar 2021 auf der EU-Plattform „SIMAP“. Nach erfolgreicher Prüfung der Eignungskriterien von zahlreichen Firmen wurden die Verhandlungsrunden durchgeführt und der Zuschlag schlussendlich an den geeignetsten Bewerber erteilt.

Eine Veröffentlichung bzw. Benennung der bewerbenden Unternehmen und ihrer Produkte würde die in einem derartigen Vergabeverfahren übliche zugesicherte Vertraulichkeit verletzen.

8. Aus welchen Gründen wird die Berliner Datenschutzbeauftragte nicht schon vor Beginn des Implementierungsprozesses involviert, beispielsweise auch um mögliche Alternativen abzuwägen?

Zu 8.:

Auf Einladung der Berliner Programmleitung des Programms Polizei 20/20 erfolgt regelmäßig eine Information der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) über datenschutzrelevante Vorhaben und Aspekte des Programms. Der letzte Austausch fand am 24. April 2023 statt und enthielt unter TOP 4 Informationen aus dem Programm zu VeRA (Verfahrensübergreifende Recherche- und Analyseplattform). Die Einbindung der BlnBDI erfolgt gemäß den gesetzlichen Vorgaben. Im Übrigen hat der eigentliche Implementierungsprozess noch nicht begonnen.

Im Rahmen des EU-Vergabeverfahrens war bereits die Umsetzung der rechtlich geltenden Datenschutzbestimmungen als verbindliches Ausschlusskriterium benannt, sodass lediglich Produkte von Herstellern zugelassen wurden, die diesen hohen Anforderungen entsprachen. Die Implementierungsmöglichkeiten datenschutzrechtlicher Anforderungen wurden mehrfach, insbesondere auf die durch das Bundesverfassungsgericht in seinen aktuellen Entscheidungen weiterentwickelten Anwendungserfordernissen hin, überprüft.

9. Sofern die Software Palantir weiterhin in Berlin eingesetzt werden soll: Wie wird sichergestellt, dass keine Daten von Dritten, die nicht als Störer*innen in Betracht kommen (zB Zeug*innen, Verfahrensbeteiligten oÄ) oder Personen abgefragt werden, die einen herausragenden Grundrechtsschutz genießen (Presse, Journalist*innen etc.). Kann durch den Einsatz von Palantir nur auf eigene Datenbanken der Polizei Berlin zugegriffen werden oder auch auf externe, gegebenenfalls frei zugängliche Quellen wie soziale Netzwerke? Für den Fall, dass auch auf externe Dateien zugegriffen werden kann: Wie positioniert sich der Senat zu dem Umstand, dass durch die Abfrage von frei zugänglichen Daten untereinander bzw. in Verknüpfung mit polizeilich gespeicherten Daten umfangreiche Persönlichkeitsprofile angefertigt werden können?

Zu 9.:

Die personenbezogenen Daten von Dritten werden im polizeilichen Vorgangs- und Fallbearbeitungssystem gemäß den gesetzlichen Vorgaben dokumentiert, gekennzeichnet und unterliegen festen Speicher- bzw. Löschfristen. Die Software von Palantir (VeRA) kann somit ausschließlich die Daten nutzen, die im Rahmen einer Einzelabfrage im jeweiligen System auch erlangt werden können.

Die Analyse- und Auswertepattform hat keine Verbindung zum Internet. Es wird ausschließlich auf behördliche Daten gemäß bestehender Berechtigungen zugegriffen.

Durch die Implementierung höchster sicherheitstechnischer Hürden ist zudem gewährleistet, dass

- Änderungen und Datenmanipulationen in den Quellsystemen ausgeschlossen sind, da polizeiliche Datenquellen an die Analyseplattform ohne Rückkopplung angebunden werden („Daten-Einbahnstraße“)

- der Auftragnehmer Palantir keinen technischen Zugriff auf die gelieferte Software im Rechenzentrum haben wird und
- der Betrieb ausschließlich in einem abgeschotteten polizeilichen Rechenzentrum erfolgen wird.

10. Sofern Palantir in Berlin eingesetzt werden soll, inwiefern wird sichergestellt, dass andere Akteure wie das amerikanische FBI oder die Herstellerfirma keinerlei Zugriff auf Berliner Daten bekommen?

Zu 10.:

Da der Softwarehersteller Palantir keinen technischen Netzwerkzugriff auf das Rechenzentrum haben kann, ist eine Ausleitung an Palantir selbst oder andere Akteure ausgeschlossen.

11. Es heißt von Seiten des Senats zudem "es können ausschließlich Daten genutzt werden, die rechtmäßig vorhanden sind": Inwiefern soll der rechtmäßige Bestand von Daten regelmäßig und zuverlässig überprüft und sodann korrigiert und gelöscht werden angesichts der immensen Datenmengen? Inwiefern wird sichergestellt, dass die (Herkunft bzw. ursprünglich Erhebungszweck der) Daten ausreichend gekennzeichnet werden?

Zu 11.:

Rechtmäßig vorhandene Daten sind Informationen, die gemäß den geltenden (datenschutz-) rechtlichen Bestimmungen erhoben, gespeichert und verwendet werden.

Die Speicherdauer dieser Daten ist in den einschlägigen rechtlichen Bestimmungen festgelegt und deren Einhaltung durch technische Umsetzung gewährleistet.

Durch die Software von Palantir-(VeRA) sind sowohl die Kennzeichnung von Daten als auch die Vorgaben zur hypothetischen Datenneuerhebung realisierbar.

12. Da der Senat im Rahmen der Frage 5 in Anfrage 19/17787 nicht dezidiert auf die Risiken der Diskriminierung und Stigmatisierung beim Einsatz der Palantir-Software geantwortet hat: Wie positioniert sich der Senat zu dem Umstand, dass Palantir menschenrechtliche Standards nicht einhalte? Inwiefern hat der Senat berücksichtigt, dass von etwaigen rassistischen Vorurteilen geprägte Daten ungeprüft in die Analyse einfließen und auf diese Weise auch in Zukunft disproportional von Kontrollen betroffen sein könnten?

Zu 12.:

Die Missachtung von menschenrechtlichen Standards durch Palantir ist dem Senat nicht bekannt.

Die Daten in den polizeilichen Basissystemen selbst sind nach den rechtlichen Vorgaben erhobene und gespeicherte Fakten, ohne jedwede inhärente Eigenschaften über den

erhobenen Wert hinaus. Die Polizei Berlin erfasst Daten nach rechtsstaatlichen Grundsätzen und Normen.

Berlin, den 21. März 2024

In Vertretung

Christian Hochgrebe
Senatsverwaltung für Inneres und Sport