Automatisierte Datenauswertungen der Polizei oder auch: KI und das Grundgesetz – über die mündliche Verhandlung am BVerfG vom 20.12.2022

Jan Keesen 2022-12-23T13:58:45

von
ANNA MICHEL und DENISE MÜLLER

Welche verfassungsrechtlichen Vorgaben gelten für Befugnisnormen, die den Gefahrenabwehrbehörden automatisierte – und sogar „intelligente“ – Datenauswertungen bzw. -analysen erlauben? Am Bundesverfassungsgericht sind aktuell zwei Verfahren anhängig (1 BvR 1547/19, 1 BvR 2634/20), in denen es um Rechtsgrundlagen zur automatisierten Datenverarbeitung (§ 25a Abs. 1 Alt. 1 HSOG, § 49 Abs. 1 Alt. 1 HmbPolDVG) geht. In der Mündlichen Verhandlung am 20.12.2022 wurden die technischen und tatsächlichen Hintergründe komplexer Datenverarbeitungen zur Gefahrenabwehr detailliert beleuchtet. Rechtlich wurde vor allem über den Zweckbindungsgrundsatz und die Bestimmtheit diskutiert.

1. Verfahrensgegenstand

Im Zentrum der verfassungsrechtlichen Prüfung stehen zwei fast identischen Normen: § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG. Demnach darf die Polizei in „begründeten Einzelfällen (in polizeilichen Dateisystemen) gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung“ zur Datenauswertung verarbeiten, wenn dies „zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten“ erforderlich ist. Einige Rechtsanwält*innen, Journalist*innen und Aktivist*innen haben unter Federführung der Gesellschaft für Freiheitsrechte dagegen geklagt. Die

Verfahrensbevollmächtigten Prof. Singelnstein und Prof. Golla kritisieren, dass die technikoffenen Rechtsgrundlagen zu weit gefasst seien, um die damit verbundenen, tiefen Grundrechtseingriffe rechtfertigen zu können. Die Normen enthielten keine angemessenen Verfahrensvorschriften zu Transparenz und Kontrolle und würden keine Anforderungen an die Qualität der eingespeisten Daten formulieren, um beispielsweise Diskriminierungen oder die Weiterverarbeitung fehlerhafter Daten zu verhindern (Hessen S. 70 ff., Hamburg S. 61 ff.). Einführend erklärte die Berichterstatterin Prof. Britz, das Gericht habe teilweise „Bedenken an der Zulässigkeit“ und beschränke die Prüfung deshalb auf die Eingriffsschwellen, weshalb die von den Beschwerdeführern geäußerten Zweifel an der Qualität der eingespeisten Daten und die verfahrensrechtliche Flankierung durch Transparenz- und Kontrollvorschriften im weiteren Verlauf keine Rolle spielten.

2. (Noch) Kein Einsatz von KI

In Hessen wird von der automatisierten Datenauswertung seit Jahren Gebrauch gemacht, während es in Hamburg bisher noch keinen Anwendungsfall gibt. Bereits seit 2017 arbeitet Hessen mit „hessenDATA“, einer Software des Anbieters Palantir. Mit § 25a HSOG wurde daher in 2018 lediglich eine bereits bestehende Praxis kodifiziert. Bei hessenDATA handele es sich um eine Analysesoftware, die es ermögliche, Daten aus insgesamt sieben separaten „Datentöpfen“ (die sog. „Quellsysteme“) gleichzeitig auszuwerten, erörterte ein Vertreter der hessischen Landesregierung. Als Quellsysteme angeschlossen seien unter anderem das Fahndungssystem POLAS, das Vorgangsbearbeitungssystem ComVor, das Fallbearbeitungssystem eFBS und eine Datei mit erhobenen Verkehrsdaten. HessenDATA sei nicht an das Internet angebunden; es handele sich dabei explizit nicht um ein lernfähiges, intelligentes System. Vielmehr wird die Software wie eine Suchmaschine genutzt, bei der die Ermittlungen von Polizeibeamten angestoßen und in unterschiedlichen Quellsystemen gespeicherte Daten sichtbar gemacht werden. Die verwendeten Suchbegriffe seien grundsätzlich mit bestimmten Personen oder Orten verknüpft und hätten daher einen Bezug zu der drohenden Gefahr bzw. Straftat. Bei der Einrichtung der Software wurde unter Einbindung des Landesdatenschutzbeauftragten (§ 25a III HSOG) festgelegt, dass hessenDATA im Phänomenbereich Terrorismusabwehr, Staatsschutz sowie schwere und organisierte Kriminalität eingesetzt werden kann. Insgesamt 2099 Ermittler sind berechtigt, die Software zu nutzen, 50 von ihnen können auf die besonders sensiblen Verkehrsdaten zugreifen. In 2020 gab es insgesamt 14.000 Suchanfragen in hessenDATA. Mit dessen Unterstützung könnten Polizisten die zerklüftete polizeiliche Datenlandschaft schneller erschließen, betonten die Ermittler. Als Beispiel wurde ein Fall genannt, bei dem ein Mitglied der sog. „Reichsbürger“-Szene verhaftet wurde, nachdem er zuvor bei einem Verkehrsunfall eine Telefonnummer angegeben hatte. Mit Hilfe von hessenDATA konnte eine Verbindung zwischen der bekannten, aber zunächst nicht zuordenbaren Telefonnummer und den bei dem Verkehrsunfall genannten Daten wie der Telefonnummer inklusive des Klarnamens und Aufenthaltsorts der Person gezogen werden, die schlussendlich zu einem Haftbefehl geführt hat.

3. Diskussion um das Eingriffsgewicht

Für die verfassungsrechtliche Beurteilung der Eingriffsschwelle ist das Eingriffsgewicht entscheidend. In diesem Zusammenhang interessierte den Senat, ob die Norm die klassische Polizeiarbeit lediglich effektiver und schneller macht oder ob auf ihrer Grundlage Muster sichtbar werden können, die selbst geschulte Polizisten nicht erkennen können. Einerseits betonten die Landesregierungen, dass es sich lediglich um die Zusammenführung von bereits rechtmäßig erhobenen, landeseigenen Daten handele. Es entstünden keine neuen personenbezogenen Daten, was unter anderem dadurch verdeutlicht werden könne, dass das Ergebnis einer Recherche in hessenDATA nicht gespeichert werde. Insgesamt sei das Eingriffsgewicht „moderat“. Demgegenüber argumentierten die Beschwerdeführer und die Datenschutzbeauftragten (Prof. Kelber, Prof. Roßnagel, Thomas Fuchs), dass es sich bei den durch hessenDATA ermöglichten Schlussfolgerungen um neue personenbezogene Daten handelt, die in den Quellsystemen erfasst werden können und damit ebenfalls in hessenDATA erscheinen. Die Normen hätten daher auch ohne den Einsatz von KI schwere Grundrechtseingriffe zur Folge. Letztlich wird entscheidend sein, wessen Ansicht der Senat teilt.

4. Aufhebung der Zweckbindung?

Die Fragen der Richter*innen zielten wiederholt auf das Problem ab, ob und wie bei automatisierten Datenauswertungssystemen sichergestellt werden kann, dass der Zweckbindungsgrundsatz gewahrt wird. Obwohl die Normen selbst keine Regelungen dazu enthielten, könne man aus den allgemeinen Datenschutzbestimmungen der Gesetze ableiten, dass der Zweckbindungsgrundsatz gelten solle. Praktisch stelle sich jedoch die Frage, ob eine strenge Zweckbindung überhaupt im Sinne derjenigen sein könne, die das Tool effektiv nutzen wollten, so Britz. Letztendlich stellte sich heraus, dass die Daten in den Quellsystemen aus technischen Gründen nicht gekennzeichnet werden können, sodass der Zweckbindungsgrundsatz aktuell (anders als die gesetzlichen Regelungen es vermuten lassen) tatsächlich nicht gewahrt wird. Problematisch ist dies insbesondere, wenn sensible Verkehrsdaten, die ursprünglich nur unter Wahrung hoher Voraussetzungen erhoben werden durften, ohne Kennzeichnung in der Analysesoftware auftauchen und zu anderen Zwecken weiterverarbeitet werden.

5. Weite der Norm

In § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG ist lediglich die Rede von einer „automatisierter Anwendung zur Datenanalyse bzw. -anwendung“. Hieraus geht nicht hervor, welche Programme zur Datenauswertung genutzt werden und welche Daten einbezogen werden können. Daher sind die Normen nicht auf ihre bisherige Nutzung durch die Polizeibehörden beschränkt. Dies eröffne in der Zukunft auch die Anwendung von KI. Zudem kritisierte der Erste Senat, dass sich aus § 25a HSOG nicht entnehmen lasse, dass die Daten bereits bei den Polizeibehörden vorhanden sein müssten und es sich um landeseigene Daten handele. Auch das Merkmal, dass ein „begründeter Einzelfall“ vorliegen muss, sei unbestimmt. Auf kritische Nachfragen der Richterbank erläuterte eine Vertreterin der hessischen

Landesregierung, dass sich ein begründeter Einzelfall in der Praxis in zweierlei Hinsicht verdichtet haben müsse: Es müssen in der Vergangenheit möglicherweise bereits Straftaten aus dem Katalog des § 100a Abs. 2 StPO begangen worden sein und es muss in Zukunft mit der Begehung gleichgelagerter Straftaten gerechnet werden. Dies nähert sich dem Begriff der konkreten Gefahr an, findet jedoch keinen Niederschlag in der Norm. Berichterstatterin Britz resümierte, dass sich die Behörden intern ein ausgeklügeltes Regelungswerk gegeben haben und merkte an, dass es doch grundsätzlich möglich – und mit Blick auf das Demokratieprinzip wünschenswert – wäre, diese Regelungen in einem Gesetz oder zumindest in einer Rechtsverordnung oder Verwaltungsvorschrift niederzuschreiben.

6. Fazit

Obwohl die praktische Umsetzung (noch) begrenzt ist, wären wegen der offenen Ausgestaltung der Normen zukünftig unter anderem der Einsatz von intelligenter Software, die Einspeisung biometrischer Daten oder eine Form von Predictive Policing denkbar. Falls das Bundesverfassungsgericht sich mit diesen Szenarien auseinandersetzt, ist mit einem wegweisenden Urteil zur Polizeiarbeit der Zukunft zu rechnen.

Zitiervorschlag: Michel, Anna/Müller, Denise, Automatisierte Datenauswertungen der Polizei oder auch: KI und das Grundgesetz – über die mündliche Verhandlung am BVerfG vom 20.12.2022, JuWissBlog Nr. 75/2022 v. 23.12.2022, https://www.juwiss.de/75-2022/.