Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

Eingangsstatement

zu dem Symposium
„Polizeiliche Informationssysteme im Zeitalter von KI und Big Data – Notwendig für polizeiliche Aufgaben oder multifunktionaler Datenspeicher auf Vorrat?“

Bonn, 6. Oktober 2021

Es gilt das gesprochene Wort

I. Anrede

Sehr geehrte Frau Leutheusser-Schnarrenberger,
sehr geehrte Frau Hansen,
sehr geehrter Herr Prof. Bäcker,
sehr geehrter Herr Münch,
meine sehr verehrten Damen und Herren,

ich freue mich, Sie zu unserem Symposium begrüßen zu dürfen. Pandemiebedingt findet es in Form einer Hybrid-Veranstaltung statt. [Neben unseren Referentinnen und Referenten hier vor Ort nehmen derzeit über **[…]** Personen per Video-Stream teil.]

II. Einleitung

Der heutige Nachmittag steht unter dem Titel „Polizeiliche Informationssysteme im Zeitalter von KI und Big Data – Notwendig für polizeiliche Aufgaben oder multifunktionaler Datenspeicher auf Vorrat?“.

Die Verarbeitung von Informationen macht seit jeher einen Großteil der polizeilichen Arbeit aus. Seit der Einführung der elektronischen Datenverarbeitung hat sich in der polizeilichen Informationsverarbeitung sehr viel getan.

III. Bestandsaufnahme

Meine Damen und Herren, haben Sie sich einmal gefragt, ob und an welchen Stellen Ihre personenbezogenen Daten erfasst werden, wenn Sie bei der Polizei z.B. einen Betrugsversuch anzeigen oder Kontakt zu einem Kriminellen hatten?

Die IT-Landschaft der deutschen Polizeien ist historisch gewachsen und sehr unübersichtlich. Bereits das zentrale System INPOL ist für Außenstehende schwer zu verstehen. Daneben gibt es in Bund, Ländern und auf europäischer Ebene zahlreiche weitere Systeme, zum Beispiel verschiedene Fallbearbeitungssysteme, Vorgangsbearbeitungssysteme und Strafverfolgungsdateien.

Mit dem Großprojekt „Polizei 2020“ soll die Informationsarchitektur der Polizeien des Bundes und der Länder modernisiert werden. Die moderne Technik ermöglicht es, getrennte polizeiliche Datenbanken miteinander zu verknüpfen, gemeinsam zu analysieren und auszuwerten. Personenbezogene Daten von Betroffenen können so in neuen, vorher nicht relevanten Zusammenhängen verarbeitet werden. Die viel diskutierte Künstliche Intelligenz wird über kurz oder lang Einzug in die polizeiliche Arbeit finden.

IV. Ziel des Symposiums

Die Quellen-Telekommunikationsüberwachung ist oft in den Nachrichten zu hören. Auch über die Antiterrordatei wurde umfänglich diskutiert und sogar das Bundesverfassungsgericht musste zwei Mal darüber entscheiden, obwohl es sich um eine Datei für einen vergleichsweise kleinen Spezialbereich handelt. Ihnen allen würden weitere Beispiele von öffentlichen Debatten einfallen.

Die allgemeinen polizeilichen Informationssysteme fristen hingegen in der Öffentlichkeit ein Schattendasein. Das ist verwunderlich, denn alles, was in der informationellen Arbeit der Polizei passiert, betrifft tagtäglich sehr viele Menschen.

In den polizeilichen Datenbanken finden sich keineswegs nur verurteilte Straftäter. Personenbezogene Daten werden in der Regel auf Verdachtsbasis verarbeitet.

Aber auch Personen, die selbst überhaupt keinen Anlass als vermeintliche oder wirkliche Täter hierzu gegeben haben, wie Zeugen oder Geschädigte, sind Gegenstand polizeilicher Datenverarbeitung.

Einerseits bestreitet niemand – gerade auch nicht wir Datenschützer: Die Polizei benötigt Daten für ihre Arbeit.

Anderseits lässt sich aber ebenso wenig bestreiten: Polizeiliche Datenbestände können für die einzelne Person ein Risiko darstellen. Einmal gespeichert, können diese Daten verwendet werden, solange sie nicht gelöscht wurden. Jede Speicherung kann dazu dienen, neue Verdachtsmomente zu generieren mit weiteren potentiellen Folgen für die betroffenen Personen.

Einträge in polizeilichen Informationssystemen können auch zu Diskriminierung und Brandmarkung führen. Besonders markantes Beispiel sind die sogenannten „Personengebundenen Hinweise“. Wer aufgrund einer entsprechenden Speicherung als gewalttätig polizeibekannt ist, muss damit rechnen, bei jedem Kontakt mit der Polizei als Gewalttäter behandelt zu werden. Auch die Verknüpfung politischer Einstellungen mit dem Verdacht krimineller Aktivitäten – also der Bereich der sogenannten politisch motivierten Kriminalität – kann sensibel sein, gerade dann, wenn die Grundlage der Speicherung lediglich ein Verdacht ist.

Bei einer optischen Erfassung einer Demonstration durch die Polizei kann zum Beispiel niemand sicher sein, ob seine/ihre Teilnahme anonym bleibt bzw. ob seine/ihre durch die Teilnahme ausgedrückte politische Haltung polizeilich erfasst wird.

Das Bundesverfassungsgericht formulierte einst treffend: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.

Vor diesem Hintergrund ist es mir ein wichtiges Anliegen, die Thematik der polizeilichen Informationssysteme aus ihrem Schattendasein heraus- und einer breiten öffentlichen Debatte zuzuführen. Und da gibt es einiges an Diskussionsbedarf.

- Wie lassen sich die Einhaltung datenschutzrechtlicher Grundsätze, wie Zweckbindung, Transparenz und Datenminimierung, in polizeilichen Informationssystemen gewährleisten?

- Wo liegen die ethischen und rechtlichen Grenzen des Einsatzes Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr?

- Wie viel Datenverarbeitung und welche Formen der Datenverarbeitung zu Zwecken der Strafverfolgung und der Gefahrenabwehr sind gesellschaftspolitisch verantwortbar?

V. Datenschutz ist Freiheitsschutz

Meine Damen und Herren,

Ein gewöhnlich schlecht unterrichteter und schlecht recherchierender Journalist hat uns Datenschützer vor kurzem wieder einmal als „Täterschützer“ diffamiert und u.a. gefordert, wenn auch nach seiner Meinung wohl satirisch, mich offiziell als „Gefährder“ einzustufen.

Statt derartigem dümmlichen Gebrabbel würde ich mir viel lieber mehr Sachlichkeit wünschen. Denn letztendlich steht hinter dem Ganzen eine handfeste Auseinandersetzung.

Das geht schon mit den Begriffen los. So dürfen „Täter“ und „Beschuldigte“ nicht in einen Topf geworfen werden. Wenn die Polizei vor Ort erscheint, zwei Männer mit blutigen Lippen antrifft, bei denen beide sagen: „der andere hat angefangen“ – Wer ist denn dann der Täter?

Daten betreffen oft nur Verdachtslagen. Schon deshalb ist eine differenzierte Sichtweise nötig! Auch der Gedanke der Resozialisierung fordert dies von uns. Soll eine Jugendsünde einem Menschen ewig nachhängen? Ich meine: Nein!

Datenschutz ist daher kein Täterschutz, Datenschutz ist Freiheitsschutz! Er steht den Polizeibehörden nicht im Wege, wenn sie in angemessenem Umfang Daten verarbeiten. Er setzt aber rechtsstaatliche Grenzen. Genau darum geht es heute.

Ich freue mich auf einen interessanten Diskurs und wünsche uns zahlreiche Anregungen, die sich in der Praxis bewähren sollten!

Ich danke Ihnen für Ihre Aufmerksamkeit.