Lea Voigt

polizei 2020

Auf dem Weg zum »gemeinsamen Datenhaus der deutschen Polizei«.

Die aktuellen Reformen der Polizeigesetze auf Bundes- und auf Landesebene werden vorrangig unter dem Gesichtspunkt neuer polizeilicher Befugnisse und der Vorverlagerung polizeilichen Handelns durch die Einführung des Begriffs der *drohenden Gefahr* diskutiert. Es lohnt sich aber ebenso ein Blick auf die übrigen Glieder der polizeilichen Informationsschöpfungskette, denn auch hier gibt es grundlegende Transformationen zu beobachten, die zu einem massiven Machtzuwachs der Polizei und zu empfindlichen Grundrechtseinschränkungen führen werden.

das projekt »polizei 2020«

Der *polizeiliche Informationsverbund*, den das BKA als *Zentralstelle* (§ 2 BKAG) verwaltet, besteht bisher aus einzelnen Verbund- und Zentraldateien, deren Inhalte nicht miteinander vermischt sind. Jede Datei braucht eine eigene Errichtungsanordnung (Rechtsverordnung), in der genauer geregelt ist, welche Art von Daten unter welchen Voraussetzungen und wie lange dort gespeichert werden dürfen. So gibt es beispielsweise Haftdateien (Liste der bundesweit inhaftierten Personen), Kriminalaktennachweise, phänomenbezogene Dateien (z.B. Gewalttäter Sport), Dateien mit gestohlen gemeldeten Fahrzeugen etc. Die Grenzen dieser Dateien sollen nun eingerissen werden. »Polizei 2020« nennt das Bundesministerium des Innern sein groß angelegtes Projekt, nach dessen Abschluss alle polizeilichen Daten ohne physische Barrieren zentral in einer Datenbank gespeichert sein sollen (»gemeinsames Datenhaus der deutschen Polizei«).[1] Nur durch ein sog. Benutzerrollen- und Mandantenkonzept soll sichergestellt werden, dass nicht *jeder* Beamte auf alle Daten zugreifen kann.

Den rechtlichen Rahmen des Projekts »Polizei 2020« bildet das geänderte BKA-Gesetz, das am 25. Mai 2018 in Kraft trat. Gegenüber der früheren Fassung wurde der Begriff der Datei (vgl. z.B. § 8 BKAG a.F.) für den polizeiinternen Bereich komplett gestrichen.[2] Als Grund für die Neukonzeptionierung des Datenverbunds werden die datenschutzrechtlichen Anforderungen des BKAG-Urteils des Bundesverfassungsgerichts vom 20. April 2016[3] angeführt. Es handele sich, so die Gesetzesbegründung, um ein »Grundsatzurteil zum polizeilichen Datenschutz«. Das BVerfG habe insbesondere festgelegt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung richten und sich die Verhältnismäßigkeitsanforderungen für eine solchen Zweckänderung am Grundsatz der hypothetischen Datenneuerhebung zu orientieren haben.[4] Diese Anforderungen könne man mit dem bisherigen System nicht umsetzen:

> »Die bestehende IT-Architektur des Bundeskriminalamtes, insbesondere das polizeiliche Informationssystem INPOL, ist für die Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts […] nicht ausgelegt und daher grundlegend neu zu strukturieren. Die Zentralstellenfunktion des Bundeskriminalamtes ist deshalb nicht nur vor dem Hintergrund der hohen terroristischen Bedrohungslage zu modernisieren und fortzuentwickeln. Einen wesentlichen Aspekt der Modernisierungsbestrebung stellt die Bereitstellung eines einheitlichen Verbundsystems mit zentraler Datenhaltung im Bundeskriminalamt dar, um die verfassungsrechtlichen Vorgaben auch für die anderen Polizeien des Bundes und die der Länder effektiv erfüllen zu können.«[5]

Im bereits zitierten »White Paper« heißt dies ganz ähnlich:

> »Mit der neuen Informationsarchitektur werden die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vollumfänglich umgesetzt. Damit einhergehend wird ein verbesserter, intelligenter Datenschutz verwirklicht.«[6]

Ist »Polizei 2020« also ein 254 Millionen Euro schweres[7] Datenschutzprojekt? Wohl kaum. Die vom Bundesverfassungsgericht in seinem BKAG-Urteil aufgestellten Regeln sind keineswegs neu – das lässt sich sogar unmittelbar in den Urteilsgründen nachlesen, in denen es heißt (Hervorh. nur hier):

> »Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen wie denen des vorliegenden Verfahrens kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (vgl. BVerfGE 125, 260 <333>; 133, 277 <373 f. Rn. 225 f.>; **der Sache nach ist diese Konkretisierung nicht neu**, vgl. bereits BVerfGE 100, 313 <389 f.>, und findet sich unter der Bezeichnung „hypothetischer Ersatzeingriff" auch in BVerfGE 130, 1 <34>).«[8]

Dass die Autor*innen des »Entwurfs eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes« und des »White Papers« trotzdem so tun, als habe man mit der BVerfG-Entscheidung 2016 ein neues

1 Vgl. Bundesministerium des Innern, Polizei 2020. White Paper, abrufbar unter: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/Polizei2020/Polizei2020_node.html

2 Er findet sich nur noch dort, wo es um projektbezogene gemeinsame Dateien Geheimdiensten pp. geht, vgl. § 17 BKAG.

3 BVerfGE 141, 220.

4 Bt-Drs. 18/11163, S. 1 f.

5 Fn. 4, S. 2.

6 Fn. 1, »Management Summary«.

7 Die Gesetzesbegründung geht von einmaligen Aufbaukosten für den neuen Informationsverbund in Höhe von 254 Mio. EUR aus. Hinzu kämen jährlich wiederkehrende Personal- und Sachkosten in Höhe von 29,4 Mio. EUR und ab Inbetriebnahme des Systems weitere jährliche Betriebskosten in Höhe von 33 Mio. EUR, vgl. ebenda, S. 3.

8 BVerfG a.a.O., Rn. 287.

Kapitel aufgeschlagen, hat vor allem einen Effekt: Es täuscht über den Umstand hinweg, dass man offenbar seit Jahren ein Informationssystem betrieben hat, das den längst bekannten verfassungsrechtlichen Anforderungen nicht gerecht wird.

Auch dass man diesem datenschutzwidrigen Zustand nur durch eine Zentralisierung der Datenbestände Abhilfe schaffen könne, ist eine Nebelkerze. Selbstverständlich ließe sich eine Kennzeichnung der Daten mit dem Anlass und der Art und Weise ihrer Erhebung auch in einem vertikal fragmentierten System bewerkstelligen, wenn man dies nur wollte. Triebkraft des Projekts »Polizei 2020« ist also sicher nicht der Datenschutz. Die Schaffung eines zentralen Datenbestandes verspricht vielmehr, endlich die seit den 1970er Jahren bestehenden »Kinderkrankheiten« von Inpol zu überwinden und *mehr* Daten *intensiver* und *effizienter* polizeilich nutzen zu können. Davon träumt der Polizeiapparat schon lange, nun scheinen der politische Umsetzungswille und damit auch die nötigen finanziellen Mittel endlich groß genug.

In dem »gemeinsamen Datenhaus« sollen sämtliche Daten der Länderpolizeien und der Bundespolizei vorhanden sein. Diejenigen Informationen, die »verbundrelevant« sind, nämlich für die *Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung* (§ 2 Abs. 1 BKAG), sollen allen angeschlossenen Behörden zugänglich sein. Wie genau diese Abgrenzung erfolgen wird, ist unklar. Die restlichen, nicht verbundrelevanten Daten sieht nur der einspeisende »Mandant«, was wohl bedeutet, dass die Daten innerhalb eines Bundeslandes polizeibehördenübergreifend zusammengeführt werden können bzw. sollen.

Das bayrische PAG hat – ganz im Sinne einer solchen landesweiten Datenfusionierung – schon vorgesorgt. In § 48 Abs. 2 BayPAG n. F. heißt es zwar (Hervorh. nur hier):

> »(2) Die Polizei darf die in Abs. 1 bezeichneten [aus besonders eingriffsintensiven Maßnahmen stammenden, Anm. d. Verf.] Daten an **andere für die Gefahrenabwehr zuständige Behörden** nur übermitteln, wenn dies zum Schutz eines Rechtsguts, das in der jeweiligen Befugnisnorm enthalten ist, erforderlich ist **und die Daten insoweit einen konkreten Ermittlungsansatz erkennen lassen**.«

Die Gesetzesbegründung stellt aber klar: Die gesamte bayrische Polizei ist *eine Behörde* im Sinne dieser Vorschrift.[9] Sind also z.B. Daten aus einer elektronischen Aufenthaltsüberwachung (Bewegungsprofil) in einem landesweiten Datenbestand, so können sie dort *ohne* konkreten Bezug von allen bayrischen Polizeidienststellen genutzt werden, wenn es denn um die Abwehr von (drohenden) Gefahren geht, die eine elektronische Aufenthaltsüberwachung grundsätzlich zulassen[10] (§ 48 Abs. 1 BayPAG n.F.). Derartige Regelungen bilden die Basis für eine algorithmengestützte Auswertung und Analyse der Daten, was auch erklärtes Ziel von »Polizei 2020« ist. Es geht um das »Erkennen von relevanten Zusammenhängen« und »aussagekräftige Analysen«.[11] Je mehr Informationen in einen zentralen Datenbestand eingespeist sind, desto größer der versprochene informationelle Mehrwert durch eine computergestützte Analyse. So zeigt sich, dass die Ausweitung der Informations*erhebungs*befugnisse (z. B. die elektronische Erfassung des Aufenthalts einer Person) und die Zentralisierung der Datenbestände letztlich zwei Seiten der selben Medaille sind: Es geht um den Aufbau eines möglichst großen Datenhauses.

die wachsende bedeutung biometrischer daten

Die Bemühungen, Polizeibehörden mit möglichst potenten Datensammlungen auszustatten, zeigen sich auch im Bereich der biometrischen Daten. Das neue bayrische PAG sieht erstmals eine Rechtsgrundlage für die sog. intelligente Videoüberwachung vor. Darunter versteht man die computergestützte Auswertung von Videoüberwachungsbildern. Möglich ist sowohl die Suche nach »Abweichungen«, also vermeintlich auffälligem Verhalten von gefilmten Personen z.B. an einem öffentlichen Ort, als auch die automatische Erkennung von Personen anhand biometrischer Merkmale. Durch Abgleich der Aufnahmen verschiedener Überwachungsanlagen kann das Bewegungsbild einzelner Personen nachvollzogen, es können Begleitpersonen erfasst werden. Videoaufnahmen könnten mit einem Fahndungsbestand abgeglichen und so Personen gezielt gesucht werden. Die Videotechnik entwickelt sich rasant und wird hier schon bald keine Grenzen mehr setzen. Auch die Daten zu Identifizierung von Personen sind grundsätzlich vorhanden. Alle Inhaber eines deutschen Personalausweises oder eines Reisepasses etwa müssen der ausstellenden Behörde ein biometrisches Foto überlassen. Diese hoch sensiblen Datenbestände sind allerdings bewusst nicht zentralisiert, sondern liegen bei den einzelnen Meldebehörden. So war es jedenfalls bisher.

Noch bevor Bayern eine Rechtsgrundlage für die intelligente Videoüberwachung geschaffen hat, ist der Bundesgesetzgeber aktiv geworden. Zum 15. Juli 2017 wurden das Personalausweis- und das Passgesetz reformiert. Mit dem *Gesetz zur Förderung des elektronischen Identitätsnachweises* wurde nebenbei der automatisierte Abruf biometrischer Pass- und Ausweisdaten bei den Meldeämtern für alle Landes- und Bundespolizeibehörden, die Geheimdienste, Zoll- und Steuerfahndungsbehörden ermöglicht. Nach der alten Gesetzesfassung durften nur Polizeibehörden und auch diese nur in Ausnahmefällen biometrische Daten von den Meldebehörden *automatisiert* abrufen. Nach der neuen Rechtslage sind die biometrischen Daten der meisten Bürger also quasi-zentralisiert, denn sie lassen sich nun automatisiert abfragen.[12] Ein Bild aus einer Videoüberwachung kann in eine Suche eingespeist werden, an deren Ende das System einen Namen der abgebildeten Person auswirft.[13] Dies könnte der Anfang vom Ende der Anonymität in der Öffentlichkeit sein. Es bleibt zu hoffen, dass die gegen die entsprechenden Vorschriften im Personalausweis- und Passgesetz anhängige Verfassungsbeschwerde[14] Erfolg haben wird.

Lea Voigt ist Strafverteidigerin in Bremen und Mitglied der Vereinigung Niedersächsicher und Bremer Strafverteidiger*innen. In **freispruch** # 4, Februar 2014 berichtete sie über die Datensammlungen der Polizeibehörden.

9 Vgl. die scharfe Kritik des Bayrische Landesdatenschutzbeauftragten *Petri* in seiner Stellungnahme vom 21.12.2017, S. 49, abrufbar unter https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf.

10 Gefahr oder drohende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes; Leben, Gesundheit oder Freiheit; die sexuelle Selbstbestimmung oder Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt.

11 (Fn. 1) S. 8.

12 Nach dem datenschutzrechtlichen „Doppeltürenmodell" bedarf die abrufende Behörde zwar zusätzlich einer eigenen Ermächtigungsgrundlage. Hier bestehen aber keine nennenswerten Hürden bei den jeweils einschlägigen Landes- und Bundesgesetzen.

13 Vgl. die Stellungnahme des Chaos Computer Clubs im Rahmen des Gesetzgebungsverfahrens, Kurz/Krissler/Neumann/Rieger, Stellungnahme eID, Ausschuss-Drs. 18(4)868 D, S. 8 f.

14 Abrufbar unter https://freiheitsrechte.org/home/wp-content/uploads/2018/07/2018-07-14-VB_Passgesetz-ohne-Adressen.pdf.