Thilo Weichert

Kategorie *Behörden und Verwaltung* – Laudatio

Der BigBrotherAward in der Kategorie Behörden und Verwaltung 2022 geht an die deutsche Polizei, vertreten durch das Bundeskriminalamt,

für die Art, wie personenbezogene Daten in Dateien abgespeichert und genutzt werden. Entgegen der verfassungs- und europarechtlichen Vorgaben werden die Daten in Dateien nicht oder unzureichend gekennzeichnet. Dadurch besteht die Gefahr, dass Millionen Menschen von der Polizei oder anderen Behörden ungerechtfertigter Weise als Gefährder oder Straftäter behandelt werden.

Laudator Thilo Weichert – Foto: Matthias Hornung, CC BY-SA 4.0

Als im Juli 2017 in Hamburg der G 20-Gipfel stattfand, sollte eigentlich unabhängige Presse darüber berichten. Doch dazu kam es nur eingeschränkt. 32 Presseakkreditierungen wurden zurückgewiesen, weil „Straftäter" – so die Bundesregierung – sich hierüber den Zutritt ins Innerste dieses Gipfels erschleichen wollten. Darunter ein 37-jähriger Fotograf, dessen Führungszeugnis zwar blütenweiß war, der aber 18 polizeiliche Dateneintragungen vorwies, u. a. wegen „Herbeiführung einer Sprengstoffexplosion" in der Kategorie „politisch motivierte Kriminalität" – er hatte fotografiert, während in seiner Nähe ein Feuerwerkskörper explodiert war. Die Einträge lagen teilweise 14 Jahre zurück. Ein Online-Journalist wurde abgewiesen, weil gegen ihn die haltlose Anzeige eines vorbestraften Rechtsextremisten vorlag. Auch die anderen Ablehnungen von Journalist:innen erwiesen sich im Nachhinein als unbegründet.

Das Problem der Journalist:innen bestand darin, dass sie über politische Ereignisse berichtet hatten und dadurch in den Fokus der Polizei geraten waren. Die Polizei hatte sie vor Ort erfasst – z. B. ihren Presseausweis kontrolliert – und ihre Daten gespeichert. Kein harmloser Vorgang.

Denn schon das bloße Fotografieren von Polizist:innen kann unter dem Label „politisch motivierte Kriminalität" oder „Verstoß gegen das Versammlungsgesetz" abgelegt werden – ohne dass es je zu einer Anklage, geschweige denn zu einer Verurteilung gekommen ist. Diese Label befanden sich über viele Jahre in polizeilichen Datenbanken, die über das Informationssystem INPOL bundesweit miteinander verknüpft sind.[1]

Der Sonnenstaat am Horizont

INPOL wird vom Bundeskriminalamt – dem BKA – betrieben und verbindet die Polizeibehörden des Bundes und der Länder elektronisch. Es geht zurück auf den legendären BKA-Präsidenten Horst Herold, der in den 1970er-Jahren dafür sorgte, dass das BKA massiv ausgebaut und mit moderner elektronischer Datenverarbeitung aufgerüstet wurde. Die Polizei wurde digitalisiert, zentralisiert und „intelligent" gemacht. Herold hatte damals die Vision, dass die Polizei dank elektronischer Datenanalyse schon vor dem Straftäter am Tatort sein und so die Tat verhindern könne. Er sah am Horizont den „Sonnenstaat", in dem Kriminalität weitgehend ausgemerzt sein würde. Das BKA galt weltweit als Vorreiter digitaler Polizeiermittlungen.[2]

Horst Herold wurde 1981 in den vorzeitigen Ruhestand geschickt. INPOL ist – nach einigen Überarbeitungen – bis heute in Betrieb. Inzwischen gibt es viele weitere Verbunddatenbanken beim BKA, u. a. die Anti-Terror-Datei und die Datei Rechtsextremismus – RED, an die auch die deutschen Geheimdienste angeschlossen sind. INPOL ist zwar in die Jahre gekommen, dient aber nach wie vor als Backbone für moderne Software. Die Analysemöglichkeiten digitaler Bestände sind unterdessen dank „Big Data", „Data-Mining" und sog. Künstlicher Intelligenz bei den Sicherheitsbehörden gewaltig gewachsen. Tatsächlich nutzt die Polizei inzwischen digitale Recherche- und Analysetools vom Feinsten. Und so ist es möglich, dass die Eintragung eines Polizeibeamten im digitalen Vorgangsverwaltungsprogramm in Coburg dazu beiträgt, dass die Bundesregierung einen Journalisten in Hamburg von der Berichterstattung beim G 20-Gipfel ausschließt.

Schmutzige Datenwäsche

Mit der Digitalisierung nicht mitgewachsen ist der Datenschutz – weder technisch noch rechtlich. Das hat immer wieder auch das Bundesverfassungsgericht festgestellt, u. a. mit seinem Urteil vom 20. April 2016.[3] Darin attestiert das Gericht dem BKA-Gesetz von 2008, das den Datenverbund der Polizei regelt, in vielerlei Hinsicht nicht mit dem Grundgesetz im Einklang zu stehen. Ein Grund für die Verfassungswidrigkeit war, dass es keine Vorkehrungen gegen die Zweckänderung von Daten – ich nenne das Datenwäsche – gibt.

Datenwäsche funktioniert wie folgt: Bin ich z. B. von einer polizeilichen Telefonüberwachung betroffen – unabhängig davon, ob ich wirklich ein Krimineller bin – dann setzt das den Verdacht einer schweren Straftat voraus. Dank der digitalen Vernetzung sind aber die Daten, die bei der TKÜ (Telekommunikationsüberwachung) erlangt werden, theoretisch bei jeder Verkehrskontrolle vom Rechner im Polizeiauto abrufbar. Flugs stehe ich als potenzielle Schwerverbrecher:in vor den Streifenbeamt:innen.

Um diese Datenwäsche zu verhindern, muss der TKÜ-Datensatz als solcher markiert sein. Es muss klar erkennbar sein, als was ich in der Datenbank geführt werde: als Kontaktperson, als Täterin, als Opfer, als Zeugin. Wurde gegen mich ermittelt und – weil an dem Vorwurf nichts dran war – das Verfahren eingestellt, so muss in der Datenbank meine Unschuld dokumentiert und ein Zugriff auf den Vorgang verhindert werden. Meine Daten müssen gekennzeichnet werden, damit ich nicht fälschlich festgehalten, durchsucht oder verhaftet werde – oder als Journalist:in meine Akkreditierung entzogen bekomme.

Altsysteme und Neuprobleme

Die Rechtslage verlangt genau das.

Das BVerfG hat klar geregelt, wie Polizeidaten genutzt oder weitergegeben werden dürfen. In der Folge wurde auch im überarbeiteten BKA-Gesetz[4] festgehalten, dass nicht gekennzeichnete Daten „so lange nicht weiterverarbeitet oder übermittelt werden (dürfen), bis eine Kennzeichnung … erfolgt ist".[5]

Auch die europäische Datenschutzrichtlinie für Polizei und Justiz, die seit 2018 in Kraft ist[6], fordert, dass bei der polizeilichen Datenspeicherung klar ersichtlich sein muss, ob jemand Straftäter, Verdächtiger, Opfer, Zeuge, Hinweisgeber oder Kontaktperson ist. Ebenso muss erkennbar sein, ob eine Datenspeicherung nachgewiesene Fakten dokumentiert – oder vage Verdachte bzw. persönliche Einschätzungen.

Das Problem ist, dass in den veralteten Datenbanken der Polizei eine solche Kennzeichnung oder Markierung oft nicht vorgesehen war. Kurz vor der Verabschiedung des BKA-Gesetzes im Frühjahr 2017 ist das auch dem Bundestag aufgefallen, weshalb er als Übergangsbestimmung einen §91 einfügte. Demzufolge kann bei diesen Altsystemen auf die Datenmarkierung vorübergehend verzichtet werden. Ansonsten würde die „Funktionsfähigkeit der Polizei" beeinträchtigt.[7]

Trotzdem hätte man vermuten dürfen, dass Anstrengungen unternommen werden, die Datenbanken der Polizei um entsprechende Kennzeichnungsmöglichkeiten zu erweitern. Dass nachträglich Markierungen vorgenommen werden, um den Anforderungen des BVerfG an den Datenschutz zu entsprechen. Doch das war und ist für die Polizei weiterhin viel zu viel Aufwand. Die alten Systeme wurden nicht nachgerüstet – stattdessen führt man neue Systeme ein, bei denen weiterhin die Gefahr besteht, dass z. B. Unschuldige als Gefährder behandelt werden.

Pfusch am Datenhausbau

Ein besonders abschreckendes Beispiel ist EASy GS bei der bayerischen Polizei, wo Stand Juni 2021 1.644 Fußballfans gespeichert sind, obwohl ihnen kein konkreter Vorwurf gemacht wird und ohne dass die meisten davon überhaupt etwas ahnen – allein auf Grund einer polizeilichen „Individualprognose".[8] Es genügt also schon der Verdacht, jemand könnte in Zukunft eine Straftat begehen, um in der Datei zu landen.

Das BKA vertröstet derweil auf seine Planungen für „Polizei 2020", ein gemeinsames „Datenhaus" von Bund und Ländern, das nur langsam vorankommt. 2018 wurde dazu ein 31-seitiges Whitepaper vom Bundesinnenministerium[9] veröffentlicht, in dem die nötige Kennzeichnung nur einmal erwähnt ist. Wert wird allerdings darauf gelegt, „die permanente Verfügbarkeit der Altdaten im Transformationsprozess sicherzustellen". Von Schutzmaßnahmen war schon damals keine Rede.

2020 beschwerte sich die Konferenz der Datenschutzbeauftragten, man müsse das „Datenhaus Polizei 2020" „auch an datenschutzrechtlichen Kernforderungen" ausrichten.[10] Und ein Jahr später beklagte der Bundesbeauftragte für den Datenschutz in seinem Tätigkeitsbericht, dass sich der „fachliche Bebauungsplan" für das „Datenhaus" an polizeilichen Interessen ausrichte und die rechtlichen Rahmenbedingungen ignoriere.[11]

Rendezvous mit VeRA

Heute, mehr als 6 Jahre nach dem Urteil des BVerfG, ist die Datenkennzeichnung immer noch nicht umgesetzt. Dass sich daran in näherer Zukunft etwas ändert, ist wenig wahrscheinlich. Im Gegenteil.

Im vergangenen Jahr wurde für das „Datenhaus" vom bayerischen Landeskriminalamt eine Ausschreibung für ein „Verfahrensübergreifendes Recherche- und Analysesystem" vorgenommen – abgekürzt mit dem schönen Namen „VeRA":

> *„Die Kernkompetenz dieses Systems VeRA ist der direkte Zugriff, das Zusammenführen und Auswerten von Daten aus unterschiedlichen Quellen. Das System muss sowohl bereits vorhandene polizeiliche Datenbestände als auch externe Datenquellen verarbeiten können".*

„Externe Quellen" – das kann praktisch alles sein. Bei Rasterfahndungen nach 9/11 wurden z. B. die Daten von Universitäten, dem Ausländerzentralregister und Meldebehörden zusammengeführt und abgeglichen, um sogenannte Schläfer zu identifizieren.

„Weitere Leistungsinhalte des ausgeschriebenen Systems umfassen insbesondere den Datenabgleich von internen und externen, strukturierten und unstrukturierten Datenbeständen" – also Daten, die nach bestimmten Merkmalen wie Wohnort oder Beruf geordnet sind, genauso wie simple Texte – „zum Erkennen von Zusammenhängen innerhalb der Analysesoftware".

Zusammenhänge? Nehmen wir als Beispiel Telefonverbindungsdaten, also wer hat wann mit wem telefoniert. Daraus können umfassende Kommunikations- und Beziehungsgeflechte erkannt werden, unabhängig davon, ob diese aus kriminellen oder aus ausschließlich persönlichen oder politischen Gründen bestehen. VeRA kommt auch meinen Amouren oder meinem politischen Netzwerk auf die Schliche.

Und schließlich zählt zum Anforderungskatalog „die Durchführung geografischer Auswertungen innerhalb des Systems und

die Visualisierung und der Export (mit Quellangaben) von Rechercheergebnissen sowie von Beziehungszusammenhängen zwischen Objekten."

VeRA hat also auch graphisch aufbereitete Karten, Tortendiagramme oder Verbindungslinien im Repertoire, wie sie der Ermittler im Vorabendkrimi auf sein Flipchart malt.

Kurzum: die Wundersoftware VeRA kann praktisch alles, was sich mit Daten machen lässt.

Zum Datenschutz heißt es im umfangreichen Anforderungskatalog kurz und lapidar: „Das System VeRA muss den geltenden rechtlichen, insbesondere datenschutzrechtlichen Bestimmungen entsprechen."[12]

Willkommen im Palantir-Reich

Am 7. März 2022 gab dann das Bayerische LKA stolz bekannt, dass den Zuschlag für VeRA die Firma Palantir Technologies GmbH bekommen hat, die Tochter des US-Unternehmens Palantir. Kein anderes Unternehmen habe die „sehr strengen Ausschreibungskriterien" erfüllt. Als Beleg für „höchste Ansprüche an Datenschutz und Datensicherheit" dient dabei, dass es bei VeRA von Palantir „keine Verbindung zum Internet" geben werde. Von der umfassenden Kennzeichnung der Datensätze ist einmal mehr keine Rede.[13]

Bei Palantir dürfte Datenschutz eher unbekannt sein: Der US-Mutterkonzern war für US-Geheimdienste und das Pentagon tätig und wird von Bürgerrechtler:innen und Datenschützer:innen immer wieder kritisiert. Gegründet wurde Palantir von dem umstrittenen Tech-Milliardär Peter Thiel, der rechtsextreme Politiker:innen – darunter den ehemaligen US-Präsidenten Donald Trump – finanziell unterstützt.

In Hessen und Nordrhein-Westfalen hat die Polizei in der Vergangenheit schon Erfahrungen mit Palantir-Software gesammelt. Kritik an der Beschaffung und den Funktionen einer solchen hat Ende 2018 in Hessen für einen Untersuchungsausschuss gesorgt – und, nicht zu vergessen, dem CDU-Innenminister Peter Beuth einen Big Brother Award beschert.

So kommt es nicht von ungefähr, dass der bayerische Landesbeauftragte für Datenschutz, Thomas Petri, anlässlich der VeRA-Vergabe von einem massiven Eingriff in die Grundrechte von Millionen Menschen sprach.[14]

Gefahr ohne Verzug

Der BigBrotherAward in der Kategorie Verwaltung geht aber vorrangig nicht an das Bayerische LKA, sondern an das BKA. Der Grund dafür steht in §31 Abs. 1 BKAG: „Das Bundeskriminalamt hat als Zentralstelle für den polizeilichen Informationsverbund die Einhaltung der Regelungen zur Zusammenarbeit und zur Führung des Verbundsystems zu überwachen."

Es ist das BKA, das die Gesamtverantwortung für „Polizei 2020" trägt. Es hat die Gesamtverantwortung für INPOL sowie für viele weitere Systeme, bei denen die Kennzeichnungspflicht nicht umgesetzt ist – und letztlich auch für das Data-Mining-System VeRA.

Es ist dafür verantwortlich, dass im polizeilichen Datenverbund die verfassungsrechtlich geforderten Maßnahmen nicht umgesetzt sind und deswegen weiterhin die Gefahr besteht, dass Polizeidaten unberechtigterweise gegen uns Bürger:innen zum Einsatz kommen.

Daher herzlichen Glückwunsch für den BigBrotherAward 2022 in der Kategorie Verwaltung: Bundeskriminalamt.

Anmerkungen

1 *Viele BKA-Datenspeicherungen rechtswidrig, DatenschutzNachrichten (DANA) 4/2017, 206 f.*
2 *Transatlantik 11/1980, 38; vgl. Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, S. 6 ff.*
3 *BVerfG U.v. 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, NJW 2016, 1781 ff. = NVwZ 2016, 839 ff. = DVBl 2016, 770 ff. = EuGRZ 2016, 149 ff. = K&R 2016, 395 ff. = CR 2016, 796 ff. = WM 2016, 1133 ff. = BB 2016, 1089 ff. = AnwBl 2016, 516 ff. = DÖV 2016, 530 ff.*
4 *BGAK v. 01.06.2017, BGBl. I S. 1354; zuletzt geändert durch G.v. 25.06.2021, BGBl. I S. 2099.*
5 *§14 Abs. 2 BKAG.*
6 *Richtlinie (EU) 2016/680 v. 27.04.2016, ABl. EU v. 04.05.2016, L 119/89.*
7 *BT-Drs. 18/12141, 6.*
8 *Patrick Kleinmann, Geheime Fan-Datenbank in Bayern: 1644 Fragezeichen, 18.08.2021, https://www.kicker.de/geheime-fan-datenbank-in-bayern-1644-fragezeichen-868760/artikel.*
9 *Bundesministerium des Innern, Polizei 2020 – White Paper, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=5.*
10 *DSB-Konferenz, Entschließung v. 16.04.2020, Polizei 2020 – Risiken sehen, Chancen nutzen!, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/99DSK-Polizei2020.pdf?__blob=publicationFile&v=2.*
11 *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 29. Tätigkeitsbericht 2020, 2021, Kap. 6.1 (S. 55 f.), https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.pdf?__blob=publicationFile&v=5.*
12 *Germany-Munich: Database software package, 2021/S 011-023694, Contract notice, 18.01.2021, https://ted.europa.eu/udl?uri=TED:NOTICE:23694-2021:TEXT:EN:HTML&src=0.*
13 *Bayerisches Landeskriminalamt, Noch erfolgreichere Polizeiarbeit – Zuschlag für neues Recherche- und Analysesystem der Bayerischen Polizei: Höchste Ansprüche an Datensicherheit und Datenschutz, PE v. 07.03.2022, https://www.polizei.bayern.de/aktuelles/pressemitteilungen/025971/index.html.*
14 *Knobloch, Bayerns LKA will umstrittene Palantir-Software einsetzen, 07.03.2022, Kurzlink: https://heise.de/-6541763.*