

# Vorbeugung und Aufklärung

## Daten bei der Polizei löschen lassen

In RHZ 1/16 und 2/16 hat get connected von den Schwierigkeiten erzählt, die Polizeien so machen, wenn sie Daten löschen sollen. Auch wenn diese Geschichten zunächst nicht sehr motivierend wirken: die Behörden dürfen nicht alles, und wir kriegen allzu widerrechtlich gespeicherte Daten auch weg. Während allerdings ein Auskunftersuchen maschinell erzeugt werden kann, braucht es für Löschanfragen eine auf die gespeicherten Daten zugeschnittene Argumentation. Dieser Artikel versucht, das zu deren Formulierung notwendige Grundwissen zu vermitteln.

Um überhaupt Löschung verlangen zu können, muss man wissen, was die Polizei speichert, also ein Auskunftersuchen stellen. Dabei hilft unser Auskunftsgenerator auf <https://datenschmutz.de/auskunft> – und abgesehen von albernem Spielchen mit „bestätigten“ Ausweiskopien, die manche Behörden wollen, ist das inzwischen auch recht unproblematisch (wir freuen uns dennoch über Hinweise auf obskures Zeug, das bei solchen Gelegenheiten manchmal rauskommt).

Sehr häufig löscht die Polizei aus Anlass so einer Anfrage gleich selbst. Einige wenige Behörden (vor allem das LKA Berlin) sind dabei so korrekt, vor der Löschung zu beauftragten, was denn gelöscht wurde, die Regel ist das aber leider nicht. Immerhin: Wenn alles gut geht, seid ihr Einträge der Art „Hat als Fünfjähriger mit Kerzen rumgezündelt“ (war in Bayern wirklich mal gespeichert) danach los.

Doch auch wenn die Grundrechtskenntnisse der meisten deutschen Polizeien jedenfalls im Hinblick auf ihre Datenbanknutzung im Laufe der letzten anderthalb Jahrzehnte Fortschritte gemacht haben, kommen immer noch regelmäßig Auskünfte mit Speicherungen zurück, die bei aller Erosion der Grundrechte klar rechtswidrig sind.

## Grundlagen der Löschologie

Eigentlich ist recht dicht geregelt, was Polizeien wo speichern dürfen (und was nicht): Jede Datenbank braucht eine Errichtungsanordnung mit genauer Bestimmung von Zweck und Inhalt (zum reality check vgl. get connected in RHZ 2/15). Darüber schweben Polizeigesetze der Länder oder des Bundes sowie die Strafprozessordnung, die beschränken, was Errichtungsanordnungen alles erlauben dürfen. Die Gesetze wiederum werden von ein paar Prinzipien eingegrenzt, die verschiedene Gerichte unmittelbar aus Grundgesetz oder EU-Grundrechten abgeleitet haben.

Weil die Errichtungsanordnungen von der Exekutive und die Polizeigesetze von der Legislative gemacht werden und Regierungen wie Parlamente beim Schutz der Menschenrechte ihrer Untertanen recht verlässlich versagen, bleiben in der Praxis nur die zuletzt genannten grundrechtlichen Mindeststandards als Werkzeuge für Löschanfragen.

Das hat auch Vorteile: in der Regel könnt ihr euch die Recherche nach den konkreten Regelungen sparen (ein Blick auf die Seiten zu den für euch relevanten Ländern oder Datenbanken auf datenschmutz.de schadet aber nicht) – alles, was ihr habt und mitbringen müsst, ist die Verhältnismäßigkeit, auf die Polizei angewandt auch gerne als Übermaßverbot behandelt. Demnach muss Datenspeicherung (wie alles polizeiliche Handeln) einen Zweck verfolgen und im Hinblick auf diesen drei Kriterien erfüllen:

- 1) *Eignung* – die Speicherung muss sich zum Erreichen des definierten Zwecks überhaupt eignen. So ist beispielsweise kaum vorstellbar, dass ein DNA-Profil bei der Aufklärung eines Widerstands gegen die Staatsgewalt helfen kann – dieser findet ja in direktem Kontakt statt.
- 2) *Erforderlichkeit* – der Zweck wäre ohne die Speicherung nicht oder nur wesent-

lich erschwert zu erreichen. Der Speicherzweck „Dokumentation polizeilichen Handelns“ kommt beispielsweise gut ohne präzise Personalien aus.

- 3) *Angemessenheit* – nur ganz überragende Ziele rechtfertigen tiefe Eingriffe in Grundrechte. Während also vielleicht bei menschenfressenden Kettensägenkillern die Speicherung erkennungsdienstlicher Daten ok gehen mag, ist die damit verbundene Stigmatisierung sowie die Gefahr falscher Anschuldigung für Trivialkriminalität wie Ladendiebstahl, Schwarzfahren oder Verummung nicht zu vertreten<sup>1</sup>

## Zwecke

Auf der Seite der Zwecke muss mensch ein wenig unterscheiden zwischen den verschiedenen Sorten von Datenbanken (Näheres in get connected 1/14).

Bei den *Nachweissystemen* (KAN, POLAS und Co) ist der Zweck strikt auf „Vorbeugung und Aufklärung künftiger Straftaten“ beschränkt. Dies bedeutet umgekehrt, dass zur Rechtfertigung der Speicherung die Polizei eine „Negativprognose“ stellen können muss. Dazu muss sie aus aktenkundigen „Tatsachen“ (also den gespeicherten Daten) glaubhaft ableiten, dass die betreffende Person in absehbarer Zeit auch wirklich in eine aufzuklärende oder vorzubeugende Straftat verwickelt sein wird.

Eine Demontage von Negativprognosen ist dann auch die typische Argumentation in Löscherlangen, denn Speicherungen in Nachweissystemen sind das, was mensch wirklich angreifen will. Sie sind, was bei Personalienkontrollen und Ähnlichem abgefragt wird, und dementsprechend sind Angaben über linksradikale Umtriebe oder andere Ungezogenheiten dort besonders dramatisch.

Speicherungen in *Vorgangsverwaltungen* hingegen sind in ihren Wirkungen harmloser. Konzeptionell stehen in ihnen Daten wie „wenn das Fahrrad X wieder auftaucht, rufen wir Person Y an“, und so sollte ihr Inhalt bei Personenkontrollen oder Ermittlungen nicht auftauchen (wenn das doch mal passiert, wären wir hoch interessiert an Berichten dazu). Neben der Abwicklung von Verwaltungsvorgängen ist Speicherzweck dabei noch die Polizeistatistik. Wenigstens für letzteres braucht es aber normalerweise keinen Personenbezug, und so ist es durchaus aussichtsreich, gelegentlich auf eine Anonymisierung zu drängen.

*Fallbearbeitungen* dienen der Aufklärung ganz bestimmter Straftaten und sind so für sich eher noch weniger toxisch als Vorgangsverwaltungen, auch wenn sie die irrsten Daten enthalten. Die Zahl der BeamtInnen, die diese zu Gesicht bekommen, ist nämlich normalerweise eher klein, und die Lebensdauer solcher Dateien sollte überschaubar sein. Weil dadurch auch der Grundrechtseingriff vergleichsweise moderat ist und die Polizei umgekehrt viel leichter abseitige Narrative zur Erforderlichkeit spinnen kann, sind Verhältnismäßigkeitsargumente hier schwerer anzubringen. Wenn aber solche Falldateien über Jahre gepflegt werden und gar Nachweissysteme durch die Hintertür werden, lohnt sich Widerspruch schon im Hinblick auf eine Skandalisierung solcher Missbräuche.

## Zwecklos

Natürlich gilt auch bei Löschersuchen die goldene Regel: Keine Aussagen bei der Polizei. Konkret heißt das, dass zur Begründung des Löschersuchens nur das genutzt werden soll und kann, was die Polizei schon gespeichert hat. Weitere Angaben („ich wars ja gar nicht“) oder Distanzierungen („ich wollte ja gar nicht“) sind nicht nur politisch falsch und jedenfalls potenziell gefährlich, sie sind auch nutzlos. Die Polizei und im Konfliktfall die Aufsichtsbehörde werden ausschließlich entscheiden nach dem, was die Polizei für wahr hält. Dazu wollt und könnt ihr nichts beitragen.

Insbesondere hat es keinen Wert, mit Jammern oder Reue zu versuchen, offensichtlich mit der Rechtslage verträgliche Einträge anzugreifen. Bei einer Verurteilung wegen Banküberfalls beispielsweise wird zumal bei politischer Motivation eine Wiederholungsgefahr nicht bestritten werden können. Weiter dürfte die Zahl entsprechender Speicherungen überschaubar sein, und so kann die Polizei im Falle einer einschlägigen Straftat schnell einen Satz Verdächtiger parat haben – gemeinsam ist das klar hilfreich für die Aufklärung einer angesichts der überragenden Bedeutung der Eigentumsgarantie für die FDGO erschütternd schweren Straftat. Ähnlich kann die Staatsgewalt auch für, sagen wir, die Speicherung von Fingerabdrücken bei Einbruchskriminalität argumentieren.

Als Faustregel dürfte gelten: Löscherungen halbwegs aktueller Verurteilungen jenseits von einer Handvoll Tagessätzen werden rechtlich nicht zu erreichen sein und sind nur durch Zeit, Revolution oder durchgreifende Liberalisierung des Staates zu heilen.

Auch in solchen Fällen sollten die Löschrfristen aber angemessen sein; die zehn Jahre, die die Polizei inzwischen fast standardmäßig vergibt, sind an sich für schwere Straftaten reserviert. (Grund-) Rechtslogisch sollten Speicherfristen die Verjährungsfristen der Vollstreckung angedrohter Höchststrafen nicht überschreiten; zur Orientierung sind das drei Jahre bei Sachen unter 30 Tagessätzen und fünf Jahre für Geschichten zwischen 30 Tagen und einem Jahr. Das ist zwar nur Rechtslogik, der die Polizei nicht folgen muss, und ohnehin wird sie bei wiederholten Speicherungen unter dem Schlagwort „Zuspeicherung“ und „Abbildung krimineller Karriere“ allerlei Tricks versuchen. Dennoch ist eine Korrektur allzu dystopischer Speicherfristen aussichtsreich und immer besser als der Status Quo.

## Konkret

Wie sehen Löschersuchen also konkret aus? Eine möglicher Eröffnung wäre etwas wie:

Bezugnehmend auf Ihre Auskunft vom xx.yy.20zz beantrage ich hiermit die Löschung folgender Sachverhalte aus Ihren EDV-Systemen [bzw. die Korrektur der Aussonderungsprüffristen]

Und für den Rest müsst ihr dann eben Verhältnismäßigkeitsargumentationen aufmachen. Sagen wir, die Coppers hätten euch mit einem Schlauchschal aus einer Demo gegriffen und haben nun einen personenbezogenen Hinweis LIMO sowie eben die Vermummung im KAN. Neben wir weiter an, das Verfahren wäre nach §170 Abs. 2 StPO (vgl. get connected in RHZ 2/09) eingestellt. Hier ist leider die Eignung der Speicherung zur Prävention künftiger Straftaten<sup>2</sup> nicht zu bestreiten, denn der Eintrag soll ja der Polizei eben das Filzen auf eine Personalienkontrolle hin erlauben. Stattdessen wäre die Angemessenheit anzugreifen:

Der Eintrag Nummer (x) – §17a Versammlungsgesetz zum 20.12.2018 – kann auf dem Weg zu Versammlungen regelmäßig zu Sonderbehandlungen durch Einsatzkräfte führen und sich insofern stark belastend bei der Wahrnehmung von Grundrechten auswirken. Angesichts der gerichtlich festgestellten Geringfügigkeit des Speicheranlasses ist diese Belastung dem tatsächlich belegbaren

Präventionsziel nicht angemessen. Ich bitte daher um sofortige Löschung, hilfsweise Aussonderung nach höchstens zwei Jahren.

Wenn es in diesem Fall eine ernsthafte Verurteilung gegeben hätte, könntet ihr die Löschung wohl eher vergessen – da hilft nur, das unselige Vermummungsverbot selbst anzugreifen. Hätte die Polizei aber bei der Gelegenheit noch eine ED-Behandlung gemacht und würde sie die entsprechenden Daten noch immer speichern, solltet ihr, Verurteilung oder nicht, auf die Eignung der Daten abstellen:

Meine Speicherung in der Datei ERKENNUNGSDIENST ist offensichtlich ungeeignet zur Prävention oder Aufklärung von Straftaten, für die die Polizei plausiblerweise eine Negativprognose stellen könnte. Da es hoffentlich nie soweit kommt, dass auf dem Weg zu einer Versammlung Fingerabdrücke genommen werden oder gesichtserkennende Rechner gegen die erkennungsdienstlichen Fotos abgleichen werden, kommt ein präventiver Einsatz nicht in Betracht. Das Szenario, dass der Fund meiner Fingerabdrücke auf etwa weggeworfenen Vermummungsgegenständen zur Aufklärung eines Verstoßes gegen das Versammlungsgesetz dienen könnte, ist angesichts der Praxis in der Verfolgung solcher Straftaten abseitig. Daher fordere ich die sofortige Löschung des entsprechenden Datensatzes.

Löschersuchen für Nachweissysteme werden in der Regel mehr oder minder nach diesen Mustern laufen. In Vorgangsverwaltungen mit ihren speziellen Speicherzwecken muss normalerweise anders argumentiert werden. Nehmen wir an, ein Nazi hat euch den Briefkasten gesprengt und ihr habt euch im Affekt hinreißen lassen, ihn anzuzeigen. Die entsprechende Daten Spur wird mindestens drei Jahre in der Vorgangsverwaltung stehen, und das ist, schon im Hinblick auf den Nazi-Sympisumpf in der Polizei, auch nicht ganz ungefährlich. Nachdem ihr die Anzeige aber zurückgezogen habt, könnt ihr etwa wie folgt über Erforderlichkeit argumentieren:

Zu Vorgang (x), 23.3.2019 (Anzeige gegen Rudolf H.) fordere ich die Entkopplung meiner Personalien und deren anschließende Löschung. Nachdem ich meine Anzeige zurückgezogen habe und augenscheinlich

auch keine polizeilichen Ermittlungstätigkeiten mehr stattfinden, ist keine Erforderlichkeit für das Halten meiner Personendaten mehr erkennbar, speziell nicht in meiner Eigenschaft als ehemaliger Anzeigsteller. Insbesondere können sie nicht relevant sein für die Dokumentation polizeilichen Handelns.

## Go forth

Technisch sollte Adressat des Schreibens in der Regel der Absender der Auskunft sein, also üblicherweise der/die behördliche Datenschutzbeauftragte. Das Geld für ein Einschreiben könnt ihr euch dabei sparen, denn es gibt keine Fristen, und solange Löschersuchen noch relativ exotischer Kram sind, müsst ihr ohnehin damit rechnen, nachbohren zu müssen.

Wenn die Polizei die Löschung verweigert, ist der nächste Schritt *nicht* ein (kostenpflichtiger) Widerspruch gegen den Bescheid. Er wird von der Behörde selbst entschieden, und es ist klar, was dabei rauskommt. Demgegenüber kann die Anrufung der Bundes- oder Landesbeauftragten durchaus sinnvoll sein. Ihr könnt euch auch gerne bei uns (Adresse unten) oder der Ortsgruppe in eurer Nähe rühren. Vorsorglich: Die Rote Hilfe gibt in Gerichtsverfahren dieser Art grundsätzlich keine Prozesskostenhilfe, denn das würde schnell uferlos. In Einzelfällen kann der Rechtsweg natürlich schon mal sinnvoll sein, aber wenn ihr RH-Beistand haben wollt, müssen wir das *vorher* besprechen.

Ja – Datenschutzrecht nervt mit der Art, wie wohlklingende Generalgarantien von Myriaden von Ausnahmen und Abwägungen nicht selten bis zur Nutzlosigkeit durchlöchert werden. Da ist es besonders unerfreulich, wenn AktivistInnen sich auch noch um die Einhaltung der wurmstichigen Schutzrechte kümmern müssen. In Zeiten, in denen finsterschwarze Reaktion reihenweise die ohnehin gnadenlos überforderten Datenschutzbehörden für sich reklamiert, tut es aber sonst niemand.

Datenschutzgruppe der Roten Hilfe Heidelberg  
Kontakt und Artikel-Archiv: <https://datenschmutz.de>  
PGP Fingerprint (**neuer Schlüssel**): 4FD3 B3EE  
7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1

---

<sup>1</sup>Na gut, das haben Gerichte in einzelnen dieser Fälle auch schon anders gesehen, speziell nachdem das Schröder-Kabinett mit der Wertung wiederholter Trivialkriminalität als Schwerekriminalität – z.B. für DNA-Profile – angefangen hatte. Seufz.

<sup>2</sup>Dass die Wahrnehmung des Grundrechts auf Anonymität

---

in dieser Republik immer noch eine Straftat ist, bleibt natürlich dennoch ein Skandal.