Durchblick verloren

Versuch einer Klassifikation polizeilicher EDV Anfang des 21. Jahrhunderts

> Wer schon mal eine Auskunft über von der Polizei gespeicherte Daten bekommen hat, wird darin mit großer Wahrscheinlichkeit über Sicherheitssprache wie „Auskunftssystem“, „Fallbearbeitung“, „Arbeitsdatei“ oder „Vorgangsverwaltung“ gestolpert sein. Mögen solche Wörter gelegentlich auch ein wenig wie Kriminologenbarock wirken, sie haben in aller Regel doch Bedeutung. Diese ist zwar in Zeit, Raum und der Extradimension der Polizeiarbeit nicht ganz stabil, mit ein wenig Hintergrund ist aber eine halbwegs zuverlässige Exegese möglich. Diesen Hintergrund wollen wir in diesem Artikel bieten.

Schon in der Urzeit der Polizeicomputer verbarg sich ein ganzes Ökosystem hinter den Mauern des BKA. Da waren erstens natürlich die für damalige Verhältnisse gewaltigen Datensammlungen von Versorgungsunternehmen und Vermieter_innen, die in der Rasterfahndung durchkämmt wurden. Weniger spektakulär war der Kriminalaktennachweis (KAN), der die wesentlichen Personendaten von Staatsfeinden und Bösewichtern mit Fundstellen für Kriminalakten verband und verbindet, wobei „Fundstelle“ hier bereits den Vorwurf („Widerstand und versuchte schwere Körperverletzung“) umfasst, nicht immer jedoch den Ausgang möglicherweise eingeleiteter Verfahren.

Zweck des KAN war zunächst die Beschleunigung von Abfragen, ob „etwas“ zu einer Person vorliege, und in der Tat konnten die Schleierfahndungen des deutschen Herbstes bereits „skalieren“, also weit mehr Personen auf Kriminalakten prüfen lassen, weil das zeitraubende Gekrame in Karteikästen wegfiel. Abgesehen von kurzen Einschätzungen zur Person („Personenbezogene Hinweise“ oder PHWs) hatte der KAN aber keinen Platz für all die „Spuren“ und Spekulationen, die die Polizei gerne sammelt und die umgekehrt das Bild des Inhalts von Polizeidatenbanken in der Öffentlichkeit prägen.

Dieses Bild ist dennoch nicht falsch, denn ebenfalls noch in den 70ern begann das BKA, Systeme zu betreiben, die je nach aktueller Skandallage als „Falldateien“, „Spurendokumentations/Spudok-Dateien“ oder „Arbeitsdateien“ firmierten. Eigentlich hätten diese Materialsammlungen jeweils konkrete Ermittlungen unterstützen und dann nach dem Vorbild der Rasterfahndungsdaten wieder gelöscht werden sollen. In der Anwendung mutierten sie aber rasch zu großen und langlebigen Datenhalden. Klassiker in dieser Hinsicht waren die Falldatei Rauschgift (FDR) und die Arbeitsdatei PIOS Innere Sicherheit (APIS) – das Kürzel PIOS stand für „Personen, Informationen, Objekte, Sachen“, was schon den, nun, breiten Ansatz dokumentiert.

Dateien dieser Art konnten dann etwa „Erkenntnisse“ der Art „Jürgen Trittin steht der Göttinger linken Szene nahe“ enthalten, selbst wenn die Polizei noch nicht mal eines ihrer windigen Ermittlungsverfahren zusammenstricken konnte, oder auch „Die Jutetasche der X ist bei der Demo gegen Y von Z getragen worden.“ Sammlungen dieser Art sind so offensichtlich Grundrechts- und meist auch Normalrechtwidrig, dass sie, wenn ihre Existenz und ihr Inhalt ans Licht kamen, häufig für Rügen der Datenschutzbeauftragten oder auch mal Untersuchungsausschüsse in Landtagen sorgten. Aber sie passen exakt in die Allmachts- und Kriminologenfantasien datenverliebter Polizeistrategen („Wir sind die Guten“), und so ist es wie im Splatterfilm: Zwei zersägte Zombies bauen sich zu einem neuen, noch größeren zusammen.

Gegenwart

Die Aufteilung in Datenbanken, die wie das KAN im Prinzip wie die Zettelkästen in Bibliotheken funktionieren – Nachweisdateien oder Auskunftssysteme –

und die Datenhalden der „Aufklärer“ – Fallbearbeitungen oder Arbeitsdateien – besteht auch heute noch. Rechtssystematisch hat die Aufteilung den Zweck, dass die Daten aus Auskunftssystemen breit zugänglich sein können (sprich: bei Demo-Vorkontrollen oder der Schleierfahndung abgefragt werden), weil sie vergleichsweise grundrechtsschonend sein sollen – wer da drin steht, sollte eigentlich gerichtsfest als böse und/oder revolutionär gesinnt klassifiziert und so quasi selbst schuld sein. Die Fallbearbeitungen mit ihren wüsten Spekulationen und Gigabytes von Daten treuer Staatsbürger hingegen sollen nur wenigen „Analysten“ und Spezialexpert_innen zugänglich sein.

Wenns so wäre, wärs immer noch blöd, aber selbst dieser Minimalstandard ist ständig am Erodieren. Erstens nämlich haben Gerichte der Polizei viele Freibriefe erteilt, eben doch ziemlich beliebiges Zeug in Auskunftssysteme zu packen (vgl. z.B. „Eingestellt und gespeichert“, RHZ 2/09), und die Polizei speichert dazu vieles, das sie selbst nach diesen großzügigen Maßstäben nicht dürfte (jedenfalls solange niemand hinguckt).

Zweitens bekommen Auskunftssysteme immer mehr Funktionen. Das Schengen-Informationssystem SIS beispielsweise (vgl. „Regimes an den Grenzen“, RHZ 2/10), ein ganz klassisches Auskunftssystem mit Ausschreibungen zur europaweiten Fahndung und Beobachtung, hat in seiner letztes Jahr online gegangenen Überarbeitung gelernt, mit Verknüpfungen umzugehen („X gehört zur Organisation Y“), und es lassen sich im Wesentlichen beliebige Informationen an Einträge anhängen („Unser Dossier zu X“). Zwar soll in letzteren nicht global gesucht werden können, so dass z.B. Namen, die darin erwähnt sind, etwa bei Grenzkontrollen nicht auftauchen sollten. Die Nicht-Suchbarkeit ist allerdings ein sehr ephemeres technisches Artefakt. Auf Deutsch heißt das: Es ist so brunzeinfach, eben doch durch die Anhänge zu suchen, dass eigentlich niemand an die Dauerhaftigkeit solcher Beschränkungen glaubt.

Drittens werden die Grenzen zwischen Fallbearbeitungen und Auskunftssystemen immer fließender, und nicht selten handelt es sich sozusagen nur um zwei Gesichter eines Datenbestands. Und so taucht dann eben jemand doch nur deshalb als Drogi oder Kommunist im Auskunftssystem auf, weil sie in der Fallbearbeitung als „zusammen mit Dealer B gesehen“ oder „wohnt mit Rädelsführer C zusammen“ markiert war. Gerade der Drogenbereich mit der FDR lieferte schon im letzten Jahrtausend immer wieder Beispiele für Schlüsse dieser Art. Da Drogenanwürfe im alltäglichen Umgang mit der Polizei besonders spürbar sind (sprich: filzen garantiert), fallen Datenströme aus Fall-in Nachweissysteme im dort besonders auf. Viel besser wird die Situation im Politbereich aber auch nicht sein.

Die neue Pest

Sicher war es, gemessen an der Situation, immer aufmunternd, wenn ein Besuch in der Polizeidienststelle Anfang der Nullerjahre einer Zeitreise glich: Wo sonst gab es neben Bohnerwachs noch Schreibmaschinen im aktiven Einsatz? In dem Sinn war absehbar, dass die Büroorganisation der Polizei sich ändern würde. Leider passierten diese Änderungen unter den Vorzeichen eines unkontrolliert wuchernden Sicherheitsapparats, und so wanderte mit den Schreibmaschinen auch einiges an Datenschutz auf den Müllhaufen.

Statt Gabriele deluxe und Triumph Adler helfen nun „Vorgangsverwaltungen“ (oder „Vorgangsbearbeitungssysteme“, im Folgenden kurz VVen) beim polizeilichen Papierkram. Schon ihre Anlage verrät die Überzeugung der Planer_innen, die Polizei müsse alles wissen und alles dürfen, im Zweifel auch nur, um sie vor allen anderen (also den Bösen) zu schützen. So wurden die VVen häufig allenfalls auf dem Verordnungsweg geregelt, womit es noch nicht mal eine halböffentliche Diskussion gab über die Frage, was diese Dinger können und dürfen sollen – und die stattdessen in testosteronschweren Krawatten- und Mützenrunden ausgehandelten Antworten häufig bis heute nicht öffentlich sind, vor allem in Ländern ohne Informationsfreiheitsgesetz.

Vielfach haben wir also keine Antworten auf recht elementare Fragen: Wonach kann da drin gesucht werden? Werden die Datenbestände bei Personenkontrollen abgefragt? Wie lange werden welche Einträge gespeichert? Noch nicht mal über das Auskunftsrecht hatten die Macher immer nachgedacht; so lehnte die hessische Polizei anfangs Auskünfte aus ihrer VV mit fadenscheinigen Argumenten komplett ab.

Zu den Speicherfristen ist aus machen Ländern manches bekannt; in Bayern etwa fanden sich Speicherungen wie „hat eine eine halbe Stunde lang plärrende Auto-Alarmanlage gemeldet“ noch nach fünf

Jahren (was den LfD zu einer Intervention veranlasst hat, nach der eine gewisse Verrechtlichung eingetreten ist und z.B. die Anrufe bei 110 jetzt „nur“ noch drei Monate gespeichert werden sollen). Hamburg, ursprünglicher Auftraggeber der populären VV-Software ComVor, erhält zumindest im Hinblick auf Transparenz ein befriedigend, da sie ihre VV im einschlägigen Gesetz (dem PolDVG) regeln. Personenkontrollen werden demnach drei Monate gespeichert, Anzeigen, Daten von Zeug_innen oder auch Leute, die eine Ordnungswidrigkeit begehen, drei Jahre, Straftaten und ihre Umstände fünf Jahre.

Wenn dieser Bestand tatsächlich durchsucht wird, hört die gefahrenzonierende Staatsgewalt mindestens drei Monate lang von einem Platzverweis. Wird er durchsucht? Das würden wir für eure Bundesländer gerne von euch wissen. Eigentlich sollte das nicht der Fall sein, denn Zweckbestimmung der VVen ist genau nicht Gefahrenabwehr und kann es aus den oben diskutierten Gründen verschiedener Eingriffstiefe auch nicht sein. Einerseits werden VVen aber gerne als „Quelldateien“ für die Fall- und Nachweissysteme genutzt, andererseits ist es schwer zu glauben, dass die Beamten ausgerechnet hier so viel Respekt vor Grundrechten haben sollen und auf die – zweifellos vorhandenen – Recherchemöglichkeiten in ihren VVen bei Kontolle und Ermittlung verzichten würden. Wir wären euch also sehr dankbar für Geschichten, die auf die Nutzung von VVen bei Straßenkontrollen, Gewahrsamnahmen und ähnlichem schließen lassen.

Durchblick dank EDV

VVen und Falldateien speichern potenziell viele der Daten, die traditionell in den Kriminal- und Ermittlungsakten des Staatsapparats steckten. Allein die dicken Schlucke aus der Datenpulle, die sich die Polizei inzwischen ziemlich regelmäßig genehmigt, stellen allerdings das Medium Papier-in-Leitz vor unlösbare Aufgaben. Die Soko „Bosporus“ beispielsweise, die die Mordserie des NSU konsequent nicht aufklärte, hatte rund 32 Millionen Datensätze gesammelt, Telekommunikations-Verbindungsdaten vor allem, aber auch Bezahlvorgänge, Hotelübernachtungen und vieles mehr, natürlich (fast?) alle von Unbeteiligten oder Opfern des NSU. Das ist nicht nur ein Alptraum für die Bürgerrechte, das wären auch eben mal ein paar hundert Meter Regal.

Wenn die Menschenrechtsverletzungen ein Ausmaß annehmen, das ohne Computer nicht mehr zu bewältigen ist, ist das Papier ernsthaft im Weg. Daher ist bei etlichen Polizeien die elektronische Kriminalakte (eKA) und ihre Weiterführungen Richtung elektronischer Prozessakte schwer im Kommen. Vorreiter sind hier die Bundespolizei (und mit ihr Schleswig-Holstein, das vom gleichen Software-Hersteller gefüttert wird) sowie wenig überraschend Bayern, wo bislang fast eine halbe Million Kriminalakten auf Papier geführt wurden (das macht 5% der bayrischen Bevölkerung aus). Von denen wurden in den ersten fünf Jahren des dortigen eKA-Projekts immerhin schon 80000 retrograd erfasst, also gescannt. Auch in anderen Bundesländern scheint sich etwas zu tun, die Projekte wirken jedoch nach dem, was in die Öffentlichkeit dringt, weit weniger fortgeschritten. Die Hoffnung dort ist offenbar nicht selten, dass mit ein paar groben Rechtsanpassungen die Kriminalakte durch die Summe der Einträge in VVen, die Ermittlungsakte durch eine Auswahl von Datensätzen aus Fallbearbeitungen ersetzt werden kann.

Die Verdatung der Akten nach StPO ist bürgerrechtlich spannend, weil auf diese Weise Material in den Wirkkreis des Datenschutzes kommt, das dem tiefen Staat bislang allenfalls mit großem juristischem Geschütz zu entreißen war. Und Datenschutz heißt: Auskunftsrecht. Oder na ja, es heißt: Statt einfach nur „basta“ zu sagen, müssen sich die Behörden Ausreden einfallen lassen, wenn sie ihre Geheimnisse behalten wollen. Mit halbwegs komptenten Datenschutzbeauftragten – womit wir den Bund inzwischen wohl vergessen können – wäre jetzt die Zeit, Duftmarken zu setzen für den künftigen Umgang mit personenbezogenen Daten in den elektronischen Akten. Im Zuge der Umstellung der Justiz auf EDV-Verfahren betrifft das natürlich auch Ermittlungs- und Prozessakten. Wer gerade in der Hinsicht interessante Verfahren laufen hat und Auskunftersuchen probieren will, möge unter der unten angegebenen Adresse Kontakt zu uns aufnehmen.

Was solls?

Die „Arbeitsteilung“ der Polizei-EDV ist in der bürgerlichen Rechtslogik weit mehr als Barock und Subvention für die einschlägige Industrie, denn die jeweiligen Speicherzwecke sind in den Systemen für Nachweis, Vorgänge und Ermittlung dramatisch ver-

schieden. In dieser Gedankenwelt „brauchen“ die Ermittler dringend Informationen über sexuelle Praktiken und Kommunikationspartner ihrer Verdächtigen (Fallbearbeitung), während diese Information bei einer Straßenkontrolle (Auskunftssystem) unverhältnismäßig wäre; für diese reicht die Kenntnis der laufenden und mit mindestens Restverdacht abgeschlossenen Verfahren zusammen mit den PHWs („Linksextremist“ oder „Landfahrer“ dienen danach zum „Eigenschutz“). Umgekehrt braucht der Ermittler nicht zu wissen, dass von einer verdächtigen Telefonnummer aus Partylärm in der Nachbarwohnung gemeldet wurde (Vorgangsverwaltung), während die 110-Operatorin nicht wissen sollte, dass diese Telefonnummer drei Mal aus einer Antifa-Demo heraus angerufen wurde (Fallbearbeitung).

Nun sind all die Notwendigkeiten, die sich der bürgerliche Datenschutz da suggerieren lässt, natürlich schlicht Bullshit, und wer akzeptiert, dass Verbindungsdaten oder Konstrukte rund um das schöne Wort „Extremismus“ notwendig für die Polizeiarbeit seien, ist in großer Gefahr, den Durchmarsch der Sicherheitsfanatiker nur noch wohlwollend zu begleiten.

Ganz inhaltsleer sind die Unterscheidungen aber immer noch nicht. Wenn in eurer Auskunft „Vorgangsverwaltung“ steht, könnt ihr davon ausgehen, dass die entsprechenden Daten bei jedem Besuch auf der Wache auf dem Schirm stehen; bei Demokontrollen oder im Bahnhof sollten sie aber nicht übermittelt werden. Steht irgendwie „Falldatei“, „Arbeitsdatei“ oder was ähnliches dabei, sollten diese Daten auch nicht bei anlasslosen Kontrollen auftauchen. Sehr wohl ist aber damit zu rechnen, dass Einträge in Polit-Dateien etwa bei Demo-Vorkontrollen bekannt sind, und auch, dass aus solchen Falldaten PHWs (etwa „linksextremistisch motivierter Gewalttäter“) werden. Auskunftssysteme schließlich haben in der Regel die größten Sichtbarkeiten, und daher lohnt sich hier besonders eine Bereinigung.

Die elektronische Kriminalakte schließlich – nun, sie wurde nach unserer Kenntnis bisher noch gar nicht beauskunftet. Es wird Zeit, dies zu ändern.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a