Außer Kontrolle

Fragwürdiger Datenschutz in Polizeisystemen

Die Polizei speichert viele Datensätze über Verdächtige und deren Umfeld. Prüfungen in einigen Bundesländern erbrachten verheerende Ergebnisse: Die Einhaltung von Datenschutzvorschriften wird dabei lax gehandhabt.

Von Christiane Schulzki-Haddouti

Schon ein kleines Vergehen wie Schwarzfahren reicht, um als Verdächtiger in den Dateien der Polizei zu landen. Was genau erfasst wird und wie lange Daten gespeichert werden, ist für den Betroffenen vollkommen intransparent. Polizeiliche IT-Systeme unterliegen aber wie alle anderen Systeme, die personenbezogene Daten speichern, dem Datenschutzrecht. Zusätzlich machen diverse Landespolizeigesetze einschlägige Vorgaben, wie Daten zu erheben, zu speichern, zu verarbeiten und zu nutzen sind. Die Datenschutz-Aufsichtsbehörden wachen darüber, dass all diese Vorschriften eingehalten werden. Nur sie können unabhängig jederzeit Prüfungen vornehmen, ob die Datenspeicherung den Vorschriften folgt und Korrekturen in der Verarbeitungspraxis anmahnen.

Bayerische Speicheritis

Die Ergebnisse solcher Prüfungen lassen aufhorchen. „Schluss mit der Speicheritis“ titelte die keineswegs als links-alternatives Kampfblatt bekannte „Bayerische Staatszeitung“, als Bayerns Datenschutzbeauftragter Thomas Petri die Ergebnisse seiner Prüfung des „Kriminalaktennachweises“ (KAN) gemeinsam mit dem Landespolizeipräsident Wilhelm Schmidbauer bekannt gab. Alle Landtagsfraktionen hätten sich einhellig „erfreut“ darüber gezeigt, so die Staatszeitung, dass nun endlich eine über 20-jährige rechtswidrige Datenspeicherung beendet werden soll.

Schon Ordnungswidrigkeiten reichen, um im KAN zu landen. Bei einigen Dienststellen sitzt die Enter-Taste offenbar locker, wie ein Fall aus der Praxis zeigt: Eine Frau erstattete bei einer Polizeidienststelle Anzeige, eigentlich ein alltäglicher Vorgang. Sie war emotional aufgewühlt, weil Unbekannte ihr Auto zerbeult hatten. Dafür kassierte sie erst einmal eine Strafanzeige wegen drogentypischer Auffälligkeiten. Ein Bluttest schloss Drogenmissbrauch zwar aus, die Frau blieb dennoch weiter als Drogensüchtige im KAN gespeichert. Selbst die CSU-Landtagspräsidentin Barbara Stamm

landete ohne ihr Wissen im KAN, obgleich die Staatsanwaltschaft ein Verfahren wegen Rechtsbeugung mangels Tatverdacht eingestellt hatte.

In der bayerischen KAN-Datei sind derzeit über 1,6 Millionen Personendaten von „Tatverdächtigen“ gespeichert. Sie gilt im bundesweiten Vergleich als die größte derartige Datei. Laut Gesetz muss die Polizei einen Eintrag löschen, sobald ein Verdacht ausgeräumt ist. Außerdem sind Löschfristen zu beachten: zehn Jahre für Erwachsene, fünf für Jugendliche und zwei für Kinder. Stellte die Datenschutzbehörde in der Vergangenheit aufgrund von Bürgereingaben Rechtsverstöße fest, wiegelte der Betreiber stets ab – es handele sich um bedauerliche Einzelfälle. Diese festgestellten „Einzelfälle“ waren allerdings zahlreich; in rund einem Drittel der Fälle konnte Petri bei der Polizei die Löschung von Daten durchsetzen.

Petri führte im vergangenen Jahr deshalb erstmals eine sogenannte Strukturprüfung durch, um des „Massenphänomens“ Herr zu werden. Er kam zu dem Ergebnis, dass die Daten wohl mehrerer tausend Bürger entweder unberechtigt oder zu lang gespeichert wurden.

In der „Speicheritis“ sieht Petri aber keine böse Absicht, sondern schlicht einen typischen „behördlichen Schlendrian“. Die Polizei erfuhr beispielsweise oftmals nicht, wenn die Staatsanwaltschaft ein Ermittlungsverfahren eingestellt hatte und der Tatverdacht damit wegfiel.

Bild: HmbBfDI/Thomas Krenz

Der Hamburger Datenschutzbeauftragte Johannes Caspar fordert klare Löschroutinen für Datenbestände der Polizei.

Ein weiterer Grund liegt darin, dass die Polizei Personen mit einem Restverdacht zunächst länger speichern darf. Petri verlangt daher, dass das IT-System solche Fälle automatisch wieder zur Überprüfung vorlegt. Außerdem müssten Polizeibeamte eine Kurzbegründung abgeben, wenn sie Daten über die gesetzliche Löschfrist hinaus speichern wollen. Petri hat auch schon ein nächstes Prüfobjekt im Visier: Die DNA-Datenbank will er demnächst systematisch angehen, da auch hier viele Einzelfälle auf ein möglicherweise systematisches Problem hindeuten. Auf der To-do-Liste steht auch noch die Staatsschutzdatei.

Die systematische und umfängliche Prüfung des Kriminalaktennachweises ist bislang bundesweit einmalig. In anderen Bundesländern, in denen ähnliche Verfahrensdateien gepflegt werden, gibt es bislang nur Einzelfallprüfungen, wenn Verstöße auffallen. Jeder Bürger kann direkt bei der Polizeibehörde Auskunft über gespeicherte Daten und den Zweck der Datenverarbeitung verlangen. Er kann außerdem verlangen, dass rechtswidrig gespeicherte oder nicht mehr erforderliche Daten gelöscht werden. Tut die Polizei dies nicht, kann sich der Betroffene an die Datenschutzaufsicht in seinem Bundesland wenden.

Seltene Soll-Ist-Prüfungen

Die Prüfung des bayerischen Kriminalaktennachweises zeigt, dass die Speicherdauer ein zentrales Problem ist. Auch Hamburg betreibt ein ähnliches System wie den KAN in Bayern, die CRIME-Datenbank, die zahlreiche Dateien mit verschiedenen Verdächtigengruppen enthält. Bei deren Prüfung entdeckte die hamburgische Datenschutz-Aufsicht bei der Hamburger Polizei Rechtsverstöße sowie Verstöße gegen die Errichtungsanordnung. In einer solchen Anordnung wird von Beginn an festgelegt, welche Daten zu welchem Zweck auf welche Weise verarbeitet und gespeichert werden sollen.

Die politisch umstrittene CRIME-Datei „Gruppen und Szenegewalt“ speicherte unzulässigerweise Merkmale wie „Kontaktperson“, „Punk“ oder „Türsteher“. Der Hamburger Datenschutzbeauftragte Johannes Caspar sagt dazu: „In unseren Prüfungen stellten wir fest, dass es sich in vielen Fällen nicht mehr rekonstruieren ließ, warum die Personen gespeichert waren, da die Akten dazu fehlten.“ In der Folge wurden 3794 Personen aus der Datei gelöscht. Am Ende enthielt die Datenbank nur noch 654 Personeneinträge. Rund 85 Prozent aller Datensätze mussten also entfernt werden. Daraufhin erklärte die Polizei, dass sie die Datei in der derzeitigen Form nicht mehr benötige.

Der bayerische Landesdatenschutzbeauftragte Thomas Petri setzte bei der Polizei die Löschung zahlreicher Datensätze durch.

Vor der Prüfung hatte es nur einen Datenschutzbeauftragten für die Innenbehörde gegeben. Aufgrund der desaströsen Prüfergebnisse erhielt die Polizei einen eigenen Datenschutzbeauftragten, der derzeit alle CRIME-Dateien prüft. Hamburgs Datenschutzbeauftragter Johannes Caspar bemängelt, dass seitens der IT-Verfahren klare Löschroutinen fehlen: „Das muss jetzt umgestellt werden. Im Moment müssen die Personen händisch aus dem System genommen werden. Es ist auch nicht damit getan, dass Personen automatisch gelöscht werden.“ Ähnlich wie Petri schlägt er vor, „eine Art Warnfunktion einzubauen, die man nicht einfach wegklicken kann“.

Eine weitere Baustelle ist die IT-Sicherheit. Caspar berichtet, dass er häufig bereits eine fehlende Verschlüsselung angemahnt habe. So nutze die Verwaltung zwar ein sicheres Verfahren zur Verschlüsselung des internen E-Mail-Verkehrs, doch die Polizei nicht. Eine Ende-zu-Ende-Verschlüsselung zwischen der Polizei und anderen Behörden bereite daher Probleme. Seit langem setzt er sich dafür ein, dass der Senat allen Behörden auch für die E-Mail-Kommunikation eine Standardmöglichkeit der E-Mail-Verschlüsselung bereitstellt.

Dieses Problem findet sich nicht nur in Hamburg. Auch das Bundeskriminalamt beispielsweise bietet die Kontaktaufnahme über ein Formular auf einer nicht TLS-gesicherten Webseite. Wer mit dem BKA gesichert kommunizieren will, muss die kaum verbreitete DE-Mail nutzen. Für den Austausch mit Polizeibehörden nutzt das BKA ein Intranet mit Hardware-gestützter Ende-zu-Ende-Verschlüsselung. Doch für den Austausch mit anderen Behörden setzt das BKA das eigens dazu entwickelte XTA-Verfahren noch nicht ein, das ebenfalls Ende-zu-Ende-Verschlüsselung sowie eine lückenlose Protokollierung des Datentransfers bieten würde.

Sowohl die aktuelle Prüfung in Bayern als auch die Prüfung in Hamburg zeigen jahrzehntealte Probleme auf, die sich so in allen Bundesländern finden lassen dürften. Offenbar fehlt den Datenschutz-Aufsichtsbehörden das Personal, um regelmäßig bei jedem polizeilichen Verfahren zu prüfen, ob das, was in der Errichtungsanordnung steht, dann auch tatsächlich umgesetzt wird. Sanktionen gibt es nicht, weil sie gesetzlich nicht vorgesehen sind. Hinzu kommt: Die Prüfungen erfolgen immer angekündigt, nur Einzelfälle werden innerhalb größerer Prüfungen unangekündigt angesprochen und gelöst.

Probleme seit Jahrzehnten

Dieser Tage prüfen die Aufsichtsbehörden von Bund und Ländern erstmals eine Verbunddatei, die von Bund und Ländern gemeinsam beim BKA gepflegt wird. Im Herbst sollen die Prüfergebnisse veröffentlicht werden. Aus Kapazitätsgründen konnten allerdings nicht alle Länder mitmachen. Die Antiterrordateien wurden und werden bislang von den Aufsichtsbehörden einzeln geprüft, über strukturelle Probleme tauscht man sich untereinander aus. Den Behörden wurden bislang auf ganz unterschiedliche Weise die Protokolldaten zur Verfügung gestellt: ausgedruckt, auf CD oder nur zur Einsicht vor Ort – das erschwert die Kontrolle massiv.

Inpol-neu ist ein länderübergreifendes System beim BKA, das beispielsweise überregional bedeutsame Meldungen über Straftaten und -täter verbreitet. Problematisch dürfte sein, dass es im Untersystem „Inpol-Fall“ üblich sein soll, sämtliche Personen, die irgendeine Rolle in einem Verfahren spielen, als „Kontakt- und Begleitperson“ einzustufen. Dabei sollen Informationen von unterschiedlicher Qualität einfließen, insbesondere auch nicht überprüfte Informationen aus laufenden Ermittlungsverfahren. Diese werden dann zehn Jahre lang im System gespeichert. Technisch ist „Inpol-Fall“ die Basis für die Antiterrordatei, womit das Problem hier ebenfalls auftauchen könnte.

Nicht alle Länder haben die Prüfung der Antiterrordatei schon vorgenommen. Vom Bundesverfassungsgericht wird sie in einem Turnus von zwei Jahren verlangt. In Schleswig-Holstein beispielsweise scheiterte sie bis jetzt daran, dass der für die Prüfung von Polizei und Verfassungsschutz zuständige Mitarbeiter nur über eine Halbtagsstelle verfügt und darüber hinaus weitere Aufgaben übernehmen muss. Der Landtag hatte eine personelle Aufstockung abgelehnt.

Ausweichstrategien

Keine Aufsichtsbehörde hat sich bislang mit Ausweichstrategien der Anwender befasst, die damit als unflexibel empfundene IT-Systeme umgehen. So schwirren nach Aussage eines Verfahrensentwicklers tausende Excel-, Access- und Analyst's-Notebbook-Dateien auf den polizeilichen Arbeitsrechnern herum, in denen personenbezogene Daten aus verschiedenen Bearbeitungsvorgängen kombiniert werden.

Falls dies der Fall sein sollte, ist dies wohl aus der Not geboren, da die seit Jahren angekündigten Schnittstellen zwischen den Datentöpfen der Länder nicht funktionieren. Der Bundesvorsitzende des Bunds Deutscher Kriminalbeamter (BDK) André Schulz verweist darauf, dass die Übertragung an die Bundessysteme „weitestgehend immer noch manuell" geschehe. Gegenüber dem TV-Magazin „Frontal 21" klagte der Stellvertreter von Schulz, Ulf Küch, erst kürzlich: „Wir haben kein einheitliches Datenverbundsystem mit den Polizeien in der Bundesrepublik Deutschland. Das heißt also, die bayerische Polizei ist nicht in der Lage, ihre Vorgänge oder Erkenntnisse aus Ermittlungsmaßnahmen so ohne weiteres mit Niedersachen oder Schleswig-Holstein auszutauschen." In allen drei Bundesländern werden Rola-Fallbearbeitungssysteme – heute T-Systems – eingesetzt, für die sich der BDK eingesetzt hatte, trotzdem klappt der Austausch nicht.

Die Datenschützer wissen selbst nicht, was jenseits der etablierten Verfahren geschieht. Sie gehen davon aus, dass der Informationsaustausch wohl per Papierausdruck vonstatten geht, da sie selbst aus Vertraulichkeitsgründen oftmals nur solche zur Verfügung gestellt bekommen. Was tatsächlich auf dem Arbeitsplatz eines Kriminalisten mit personenbezogenen Daten geschieht, ist nicht bekannt. Geprüft werden von der Datenschutz-Aufsicht bislang nur die IT-Verfahren, nicht aber die tatsächlichen Arbeitsprozesse.

In Sachen mobiler Kommunikation sind solche Ausweichstrategien schon lange bekannt. In akuten Gefahrenlagen wird das herangenommen, was gerade zur Hand ist: im Zweifel das private Handy mit allen möglichen schicken Kommunikations-Apps. Beim Amoklauf von Winnenden wurden in der Not private Handys genutzt, zuletzt in Hannover auch WhatsApp. Zumindest in Rheinland-Pfalz hat man sich bereits des Problems „Messenger-Dienste" angenommen: Das Landesamt für Information hat mit dem Programm „Pommes" eine eigene Messenger-Lösung für die Polizei entwickelt. Die Nutzung von WhatsApp ist dort nun ausdrücklich verboten. *(uma@ct.de)* c't