# Piff, Paff, PIAV

Der Polizeiliche Informations- und Aufgabenverbund des BKA

> Im ersten Halbjahr 2017 hat der Bundestag das Netzwerkdurchsetzungsgesetz, die Verschärfung von §113 StGB, eine StPO-Novelle, das Videoüberwachungsverbesserungsgesetz, die „Förderung des elektronischen Identitätsnachweises“ und mindestens ein Dutzend weiterer Gesetze durchgewunken, die der Polizei mehr und den Menschen weniger Rechte geben. In diesem Tsunami fast nicht aufgefallen ist eine umfangreiche Neufassung des BKA-Gesetzes, die alles umzuwerfen verspricht, was wir bisher über Datenbanken der deutschen Polizeien verkündet haben: Es liefert die Rechtsgrundlage für den Polizeilichen Informations- und Aufgabenverbund, den PIAV.

Im alten Polizeirechtsstaat war es üblich, dass das Parlament grundrechtswidrige Gesetze abnickte, das Bundesverfassungsgericht ansagte, was vielleicht gerade noch mit einem hinreichend postmodernen Verständnis von Menschenrechten verträglich sein könnte und das dann nach ein paar Jahren ins Gesetz geschrieben wurde.

Spätestens seit dem Urteil zur „Anti-Terror“-Datei (ATD) hat sich das geändert; die autoritäre Formierung der Gesellschaft ist offenbar so weit, dass der Gesetzgeber die Kritik des Verfassungsgerichts ins Gegenteil verkehren und auf die monierten Grundrechtsverletzungen noch eins draufsetzen kann, solange ein, zwei Phrasen aus den Urteilen in die Gesetzesbegründung eingearbeitet sind.

Das passierte nun auch beim BKAG. Das Gericht hatte im April 2016 die letzte BKAG-Verschärfung von 2008 in vielen Punkten verrissen, unter anderem, weil sie unter dem Mantra „Terror“ dem BKA ohne ernsthafte Beschränkungen präventive Verwanzung und Computersabotage sowie fast beliebige Verarbeitungen und Verschiebungen der erbeuteten Daten erlaubte. Leider (aber das ist mittlerweile auch Standard) beschränkte sich Karlsruhe dann auf die milde Bitte, eine Überarbeitung mit etwas mehr Rücksicht auf die Verhältnismäßigkeit (vgl. zu dieser „Vorbeugung und Aufklärung“, RHZ 1/17) vorzulegen.

Statt nun wenigstens ein bisschen zurückzustecken, hat die Regierung dem BKA noch mehr Rechte gegeben, so viele, dass das Alphabet ausging; bisher wurde in Buchstabenparagraphen zum §20 BKAG aufgezählt, wie das Amt Grundrechte verletzen darf. Mit §20y (das BKA kann Leuten die Freizügigkeit nehmen) und §20z (das BKA kann auch strafrechtlich nicht belangbaren Menschen Fußfesseln anlegen) ist im sofort wirksamen (ja! die Fesselung durchs BKA kann keinen weiteren Tag mehr warten!) Übergangsgesetz das alphabetische Limit erreicht. Was liegt da näher, als das Gesetz einfach umzustrukturieren, damit der nächste BKA-Wunschzettel nicht die Nutzung griechischer oder kyrillischer Buchstaben erfordert?

## Hypothetische Neuerhebung

Die Regierung hatte aber auch einen nichtlexikalischen Grund für die tiefgreifende Neufassung. Im Speziellen: alte Träume des BKA.

Bei fast allen diesen Träumen störte rechtssystematisch das Datenschutzprinzip der Zweckbindung, etwa, als schon Anfang der 90er Jahre das BKA seine Datenbanken unter dem Arbeitstitel INPOL-Neu revolutionieren wollte. Dabei hätte es eine „anwendungsunabhängige Einfacherfassung“ (also: alle Daten landen in einer einzigen Datenbank und werden dort auch kontinuierlich gepflegt) geben sollen und auf dieser Basis eine „dispositive Komponente“, die die Daten zur Erkennung von versteckten „Zusammenhängen“ durchkämmen sollte. Im „dispositiven“ Szenario hätte der Rechner eine Kette bauen können wie: „der gewaltbereite Autonome W. hat mal Mobiltelefon X benutzt, das Hehlerware von Y. ist. Die DNA von Y.s Bruder war aber auf dem Gebetsteppich von A., der heimlich mit B. kifft, der wiederum in einem

Terrorlager war“. Auf die Weise hätte das BKA schon ganz früh herausgefunden, wenn sich die „Extremisten“ mit der „organisierten Kriminalität“ verbünden und Armageddon nur noch durch Wiesbadener Hubschraubereinsatz aufzuhalten ist.

Einen für solche Träume ausgesprochen vorteilhaften Begriff hat das BVerfG im BKAG-Urteil geprägt: Die „hypothetische Neuerhebung“ von Daten. Danach müssen Daten, die für Zweck x erhoben wurden, nicht mehr, wie eigentlich von der Zweckbindung gefordert wird, in der Regel gelöscht werden, wenn sie für x nicht mehr nötig sind. Die Behörde muss nur rechtzeitig einen Zweck y finden, für den diese Daten auch *hätten erhoben werden dürfen*. Was den ersten Senat des BVerfG bewogen hat, mit diesem Taschenspielertrick ein Fundament des Datenschutzes effektiv auszuradieren, werden künftige RechtshistorikerInnen zu klären haben. Vielleicht war es ja wirklich und ehrlich Sorge um „Terror“ – vielleicht aber auch Resignation, denn die Polizeien löschen, solange niemand hinguckt, auch jetzt nur höchst zögerlich („kriminelle Karrieren abbilden“ ist die populärste Ausrede).

Jedenfalls: Zweckbindung ist Geschichte. Doch INPOL-Neu ist Anfang der 2000er sachlich gar nicht an ihr gescheitert. Es starb, als die Unternehmensberatung KPMG nach vielen Verzögerungen und Pannen in der Entwicklung den traditionellen BKA-Hauslieferanten T-Systems unter immer noch skandalumwobenen Umständen und Schützenhilfe von Otto Schily aus INPOL-Neu rauskantete[1]. Das, was Mitte der 2000er schließlich unter INPOL-Neu lief (spöttisch wurde schon von INPOL-Neu-Neu gesprochen), war lediglich ein Aufguss des Ländersystems POLAS und organisiert wie das alte INPOL. All die Einzeldatenbanken von FDR bis LIMO, die während der letzten vierzig Jahre in der Linken Furcht, Hass und Wut verbreitet haben, blieben uns vorläufig erhalten.

Dazu trat als Fallbearbeitung ein weiteres Ländersystem namens CRIME. Das BKA taufte es INPOL-Fall, vielleicht, um den klanglosen Abgang der „dispositiven Komponente“ etwas zu kaschieren. Wenig später holte sich das Amt noch rsCase vom privaten Hersteller rola. Das BKA ließ daran etwas rumhacken und taufte das Ergebnis b-case, während rolas Standardprodukt von Bayern (dort heißt rsCase „EASy“) aus den Ländermarkt aufrollte. Alle diese Systeme wurden zwar mit der Ansage „Data Mining“ ge- und verkauft, blieben aber aufgrund der Organisation in Einzeldatenbanken und inkompatiblen Kundenanpassungen weit hinter den Visionen von Einfacherfassung und „dispositiven“ Fähigkeiten zurück.

## INPOL-Neu-Neu-Neu

Doch die Sonnenstaats-Fantasien beim BKA versanken leider nicht im Sumpf von Profitinteressen und technischen Kompetenzschwankungen. Die alten Ideen des originalen INPOL-Neu waren schon 2007 wieder auf dem Tisch, dieses Mal mit dem Zusatzanspruch, dass der ganze Murks, mit dem die Länder ihre Nachweissysteme betreiben, ein Ende hat und die Länderdaten auch gleich ganz (und nicht nur wie gehabt nach Gusto der Länder) beim BKA landen. Projektname: PIAV.

Wie schon INPOL-Neu sollte auch PIAV wieder eine „operative“ Komponente haben, während das, was vordem „dispositiv“ hieß, nun als „strategisch“ lief. Und wie schon bei INPOL-Neu wird erstmal über PIAV-Operativ gesprochen, während das BKA zumindest gegenüber der Bundesdatenschutzbeauftragten (BfDI) hoch und heilig versprochen hat, der „strategische“ Teil solle nicht als „Big Data-Anwendung“ ausgestaltet werden. Wie das mit dem erklärten Ziel des Amts zusammengeht, den Computer „phänomenübergreifende Tat-/Täter- bzw. Tat-/Tat-Zusammenhänge“ erkennen zu lassen: Das fragen nur böse Menschen.

Das ist bei weitem nicht der einzige Punkt, bei dem das BKA einen freien Umgang mit Datenschutz und Ehrlichkeit pflegt. Die BfDI hat in ihrem Bericht für 2013/14 immerhin vier Punkte aufgezählt, über die sie mit dem BKA zu PIAV „Klarstellungen erreicht“ habe. Und macht dann mit satten 10 Punkten weiter, die „dringend geklärt werden müssen“. Nichtsdestotrotz ist die „Stufe 1“ (sic!) des PIAV-Operativ im Mai 2016 in Betrieb gegangen, und zwar spezifisch zu „Waffen- und Sprengstoffkriminalität“. In der Bundestagsdrucksache 18/10590 gibt die Regierung an, die nächste „Stufe“ mit etlichen weiteren Bereichen solle am 1.2.2018 in Betrieb gehen.

PIAV köchelt also schon mindestens zehn Jahre vor sich hin. Dennoch entblödet sich die Regierung nicht, in der Neufassung des BKAG so zu tun, als sei es die Konsequenz aus neuer EU-Datenschutzgesetzgebung und der Rechtsprechung des BVerfG. Womit beiden Unrecht getan wird, denn dieser drastische Abbau von Datenschutz wird weder von der einen noch der anderen gedeckt.

Der Bürgerrechtsabbau fängt schon bei den kleinen Details an. So gibt es beispielsweise in der Regel keine Errichtungsanordnungen mehr. Wie wir in get connected der RHZ 2/15 diskutiert haben, haben die immerhin noch eine gewisse Idee gegeben, was die Polizeien so treiben. Das BKA hingegen kann sich in Zukunft auf ein „Verzeichnis von Verarbeitungstätigkeiten“ beschränken, das absehbar *sehr* abstrakt gehalten sein wird. Angesichts dessen werden jedenfalls wir uns nicht die Mühe machen, es freizuklagen, wenn das BKA das Ding dennoch als Verschlusssache deklarieren wird (will jemand wetten?).

## Bye-Bye, DAD

Nun folgt diese „Vereinfachung“ natürlich recht zwingend aus der „anwendungsunabhängigen Einfacherfassung“. Wer die Zweckbindung auskippt, kann sich über den folgenden Abgang der Transparenz kaum wundern. Ausgenommen sind nur die weiter bestehenden geheimpolizeilichen Dateien nach dem Muster der ATD, die auch weiter Errichtungsanordnungen haben werden. Wie gesagt: Vergesst PMK-links-Z und DAD, vergesst IFIS und AFIS und schon gar die ganzen Gewalttäterdateien.

Die meisten dieser Spezial- und Falldateien wurden bisher bei einer normalen Personenkontrolle nicht abgefragt. Das war weniger menschenrechtlichen Erwägungen geschuldet, sondern wohl vor allem dem Unwillen der Wichtigwichtig-Politpolizei (oder ihrer KollegInnen bei Drogen, Falschgeld oder was immer), ihre tiefgründigen Einsichten mit den ungewaschenen Massen auf Streife zu teilen. Der bleibt natürlich, und so soll auch weiterhin nicht jedes Datum allen NutzerInnen zur Verfügung stellen. Bei INPOL-Neu lief das noch unter „komplexes Berechtigungssystem“, heute ist die Rede von „horizontalem Datenschutz“.

Details gibt das Gesetz nicht her; es steht aber zu vermuten, dass es mit der Komplexität nicht weit her sein wird und in der Regel doch alle fast alles lesen, die Arbeitsdaten einzelner Ermittlungsgruppen mal ebenso ausgenommen wie ein paar der dämlichen Phantasmen Marke CSI Wiesbaden („Terror“, „organisierte Kriminalität“, „Geldwäsche“; so war das zumindest bei INPOL-Neu geplant).

Eine weitere Ausnahme des Sichtbarkeitsprinzips ist für verdeckt erhobene Daten (also: Wanzen, Observation, Einbruch usf.) vorgesehen. Da die Maßnahmen, aus denen diese resultieren, in den verschiedenen Gesetzen speziell beschränkt sind (z.B. auf einzelne Deliktbereiche oder durch Gerichtsvorbehalt), ist für sie eine Umwidmung besonders obszön. Und darum war das Soufflieren des BVerfG mit der „hypotetischen Neuerhebung“ auch so hilfreich fürs Amt und so destruktiv für die Menschenrechte. Nicht zuletzt wird so der ohnehin kaum wirksame Gerichtsvorbehalt komplett ausgehebelt: Es ist schlicht undenkbar, dass Gerichte vor Abfragen unter dem „horizontalen Datenschutz“ von PIAV beschäftigt werden. Wenn die Polizei ein 129a auf einen Politfall klebt – und dazu gehört nicht viel –, reicht das für universellen Zugriff, und an der Stelle hat keine (geschweige denn eine gerichtliche) Prüfung der tatsächlichen Umstände stattgefunden, von Möglichkeiten der Opfer auf irgendeine Sorte rechtlichen Gehörs mal ganz zu schweigen.

Technisch jedenfalls werden die Daten im PIAV nach Quelle „gekennzeichnet“. Daten mit dem Label „Staatstrojaner“ dürften dann nicht bei Anfragen in Ermittlungen zu einfachem Schwarzfahren genutzt werden (vermutlich aber schon zu gewohnheitsmäßigem Schwarzfahren, wenn mensch die Gesetzgebung zur DNA-Analyse zum Maßstab nimmt). Die bestehenden BKA-Daten haben natürlich solche Kennzeichnungen nicht, weshalb es allerlei haarsträubende Pläne gibt, wie diese doch überführt werden können.

## Alles, was elektrisch ist

Besonders toxisch wird die Horizontalität, weil auch Spitzelberichte und abgeschnorchelte Chatprotokolle, wie alle Akten beim BKA nach neuem BKAG, elektronisch geführt werden „sollen“. Ob sie damit rechtslogisch Teil von PIAV sind oder nicht, können wir nicht ganz erkennen; derzeit jedenfalls sind die Kriminalakten, soweit sie schon elektronisch geführt werden, Teil einer INPOL-Tabelle (vgl. get connected in RHZ 4/16). Bleibt es so, unterliegen auch sie dem §84 BKAG-neu und sind damit auskunftspflichtig.

Der 84er regelt nämlich die Auskunftsrechte der Speicheropfer und überträgt die bisherige Praxis, nach der das BKA aus seinen Verbunddateien auch Auskunft über Daten erteilt, die von Länderpolizeien angeliefert wurden (und das ist die übergroße Mehrheit) auf den PIAV. Alles andere wäre natürlich auch furchtbar gewesen, doch für die in gewisser Weise PIAV-ähnlich angelegte ATD hätte eine umfassende Auskunft nach den Originalplänen wirklich eine Anfrage an alle einspeisenden Behörden vorausgesetzt.

Was das Gesetz so nicht hergibt und was vermutlich auch intern noch heftig umkämpft sein dürfte, ist die

Zukunft der zahlreichen Ländersysteme. Schon 2011 hatte der Bundestag ausgerechnet als Konsequenz aus den NSU-Aktivitäten der Sicherheitsbehörden gefordert, deren Datenbankarchitekturen zu vereinheitlichen – als hätten die Schwierigkeiten, „unterschiedliche Systeme wie EASy und INPOL Fall während einer laufenden Ermittlung zu verknüpfen“ (aus der Gesetzesbegründung zum BKAG) etwas mit der staatlichen Lethargie bei der Verfolgung des Mordkommandos des Thüringer Heimatschutzes zu tun gehabt. Halbwegs klar ist noch, dass es PIAV-Land-Systeme geben soll und wahrscheinlich schon gibt. Da die meisten Länder ihre Fallbearbeitungen bereits auf der PIAV-Basis rsCase laufen lassen, könnten die technischen Hürden da vielleicht überschaubar sein, auch wenn allerlei Software-Anpassungen auf Geheiß der LKA-Fürsten für reichlich Hader sorgen werden. Bei den Nachweissystemen mit ihren längeren Traditionen wären die Umstellungen gewiss noch drastischer.

Unklar ist weiter, ob die Datenhaltungen von PIAV-Land physikalisch in Wiesbaden liegen sollen – Sorgen der BfDI, das BKA könne künftig mehr Daten sehen als es dürfe, deuten dies an. Ob sich die Länder dann aber von ihren überkommenen POLAS-, @rtus-, Polygon-, oder was-immer-Nachweissystemen trennen werden? Das BKAG scheint das jedenfalls nicht kategorisch zu verlangen, und dann wäre PIAV aus Ländersicht wohl kaum mehr als eine nach auch schon jahrzehntelangem Rumgepfriemel schließlich funktionierende Schnittstelle zum automatischen Datenaustausch mit dem BKA. Sowas gab es zwar bisher auch schon (Codename „BLDS“), aber offenbar funktionierte das nur für eine Minderzahl der Länder-Datenbanken.

Das BKA hingegen scheint eher davon zu träumen, die ganze EDV der Länder zu organisieren. Womit sich dann aber die Frage stellt, was mit den Vorgangsverwaltungen der Länder passieren soll, in denen die Polizeien z.B. Anrufe wegen toter Vögel speichern. Zwar ist wahrscheinlich, dass die Data Miner vom BKA auch diese Daten gerne hätten („aus Häufungen von toten Vögeln könnten wir ja vielleicht auf Bombenwerkstätten schließen“), doch sind die Verfahren in den einzelnen Ländern schon wegen der unterschiedlichen Polizeigesetze kaum realistisch zu vereinheitlichen. Noch dazu haben etliche Länder ihre Nachweissysteme und ihre Vorgangsverwaltungen integriert (was in sich natürlich auch schon ein Skandal ist). Dass sie das nun wieder entflechten sollen, ist schon industriepolitisch schwer vorstellbar.

Prognosen über den Ausgang des großen PIAV-Plans sind also schwierig, und damit auch dazu, was beim Zünden von „Stufe 2“ (und damit der Verwaltung ernsthafter Datenbestände in PIAV) am 1.2.2018 wirklich passiert. Das neue BKAG tritt am 28.5.2018 in Kraft, und dann sollte INPOL Vergangenheit sein. Auf der anderen Seite hat das BKA nie viel auf Gesetze gegeben, wenn es um seine EDV ging.

Und dann wäre da noch der Data-Mining-Alptraum PIAV-strategisch. Einfach nur hoffen, dass sie es wie bei INPOL-Neu unter tätiger Mithilfe einer Unternehmensberatung wieder in den Sand setzen, ist wahrscheinlich kein guter politischer Umgang mit den düsteren Vorhaben aus Wiesbaden. Dennoch: Wo ist McKinsey, wenn mensch sie mal braucht?

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

PGP Fingerprint: 4FD3 B3EE 7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1

[1] Nachhaltig war das allerdings nicht, denn der Lieferant von PIAV, rola security solutions aus Oberhausen, wurde im Zuge der PIAV-Einfädelung wiederum von T-Systems übernommen. Manchmal hilft eben Kapitalismus doch dem Datenschutz.