

Das Prinzip der Verfügbarkeit

Europol, Prüm, VIS und kein Ende

Die EU-Regierungen haben sich nicht nur SIS gegeben, um ihre und vor allem fremde BürgerInnen sicherzustellen. Es gibt auch eine übergreifende Polizei, die sich als Verschiebebahnhof für Daten versteht, eine Art Superstaatsanwaltschaft, eine Sammlung von Fingerabdrücken von AsylbewerberInnen, munteren Austausch zwischen den nationalen Polizeien und natürlich große Pläne. Das passende Motto der Veranstaltung: „Prinzip der Verfügbarkeit“ -- was würde Klaus Theweleit dazu sagen?

Die InnenministerInnen der EU-Staaten beschließen seit 2000 Fünfjahrespläne zur Ausweitung von Repression und Kontrolle im Unionsinneren und zu deren Projektion jenseits der EU-Außengrenze. Das „Prinzip der Verfügbarkeit“ kommt als Begriff aus dem Vorgänger des seit diesem Jahr geltenden Stockholmer Programms, nämlich aus dem Haager Programm von 2004. Das Prinzip sagt grob: Die Polizeien der Mitgliedsstaaten sollen sich gegenseitig so weit Zugriff auf ihre Datenbestände geben, wie das zur „Erfüllung ihrer Aufgaben“ nötig ist.

Bereits im ersten Teil dieses Zweiteilers zur EU („Regimes an den Grenzen“, RHZ 1/2010) hatten wir den Konflikt zwischen der Verlockung fremder und der Behauptung eigener Machtmittel als Fundament so mancher EU-Merkwürdigkeit beschrieben. Natürlich bleibt es auch bei der Verfügbarkeit dabei: Alle möchten gerne wissen, was die anderen haben, diesen aber nur möglichst oberflächliche Blicke in die eigenen Karten zugestehen.

Prüm

Um zehn Parteien mit solchen Interessen zusammenzubringen, bedarf es Suggestions- und Erpressungskraft, zusammenfassend auch als Diplomatie bekannt.

Auch wenn es bei Dauersirene Wolfgang Schäuble kaum zu glauben ist, er hatte nicht zu knapp davon, als er seine KollegInnen aus Spanien, Frankreich, Österreich und den Beneluxstaaten 2007 in der ehemaligen Kreisstadt Prüm in der Eifel versammelte und sie ihren Behörden gegenseitigen beschränkten Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten einräumen ließ. Inzwischen ist dieser Vertrag von Prüm Acquis, also Pflichtprogramm für EU-Mitglieder.

Der Prüm-Mechanismus soll wie folgt funktionieren: Die Polizei in Rosenheim nimmt einem Punk Fingerabdrücke ab. Beim Abgleich im Computer kreuzen die Beamten nicht nur das BKA in Wiesbaden an, sondern vielleicht auch noch Österreich und Tschechien. Dann geht der Fingerabdruck an dortige Kontaktstellen, die automatisch mit „Täter“, „Tatortspur“ oder „nichts“ antworten, je nach dem, ob und als was der Fingerabdruck in ihren Datenbanken auftaucht. Weitere Daten werden in diesem automatischen Verfahren nicht übermittelt.

Die Fairness des Prüm-Deals besteht darin, dass beide Polizeien neue Daten haben: Die BRD weiß, dass der Punk in Österreich geführt wird, die Österreicher, dass er in Rosenheim aufgeschlagen ist. Die Kontaktstelle in Wien kann daraufhin die Übermittlung des eigentlichen Datensatzes -- sagen wir, der gefangene Punk hätte mal einen Haider-feindlichen Aufkleber in St. Pölten geklebt -- veranlassen. Sie darf es nach Prüm aber auch lassen, etwa in der Hoffnung, der Punk möge seine weiteren Aufkleber bei den Piefkes verpappen.

Analog funktioniert das für DNA-Profile, während bei Kraftfahrzeugen die ausländischen Behörden direkt Autonummern eingeben können und zurückkriegen, auf wen das Fahrzeug zugelassen ist (hier konnte Prüm auf ein bestehendes Netzwerk namens EUCA-RIS zurückgreifen).

Etwas jenseits des üblichen Prüm-Betriebs fällt der

speziell auf den Politbereich getrimmte Artikel 14 des Vertrags von Prüm auf, nach dem vor „Großereignissen“ weitgehend beliebige Daten über „Gefährder“ angefragt und übermittelt werden können. Als Beispiel nennt der Vertrag „Tagungen des europäischen Rats“ -- Göteborg muss wirklich ein schlimmer Schock gewesen sein. Die übermittelten Daten, neben Identifikationsdaten auch das, was in Kreisen der Staatssicherheit als „Tatsache“ durchgeht, können vom Empfängerland bis zu ein Jahr aufgehoben werden.

Diese Artikel 14-Geschichte wäre ein größerer Aufreger, wenn nicht auch §14 des nationalen BKA-Gesetzes (und ähnliche Regelungen in Geschwistergesetzen) das internationale Verschieben von Daten für ähnliche Zwecke erlauben würde. Prüm hilft aber, Konfusion zu schaffen: Die Daten etwa, auf deren Grundlage französische Behörden KöchInnen und andere nicht zum NATO-Jubiläum letztes Jahr einreisen ließen (dabei ging es um insgesamt weniger als 1000 Datensätze, die das BKA selbst teilweise aus dem Ausland hatte), wollte die Bundesregierung in einer Antwort auf eine Anfrage „grundsätzlich“ nach nationalem Recht, in einem Bericht an den Innenausschuss „auf Grundlage und nach Maßgabe“ von Prüm verschoben haben.

Überlast

Der jetzt unter Prüm-Flagge segelnde große Handel mit biometrischen Daten war Anfang des Jahrtausends eigentlich für den SIS-Nachfolger SIS II vorgesehen gewesen. Schäuble hat Prüm durchgedrückt, weil die massiven Verzögerungen von SIS II 2007 abzusehen waren und er im Falle eines -- immer noch möglichen -- völligen Scheiterns ein Plan B in Petto haben wollte.

Die Ausgestaltung des Plan B hat aber recht offensichtliche Schwächen. Bei einem SIS-ähnlichen System nämlich brauchen 27 Staaten 27 Programme, die ihre nationalen Polizeisysteme an das Zentralsystem anbinden (tatsächlich sind es weniger, weil manche Staaten keinen nennenswerten Polizei-Industriellen-Komplex und drum Ausrüstung von anderen Staaten haben).

Bei einem System vom Prüm-Typ muss hingegen jeder mit jedem reden, was bei 27 Mitgliedsstaaten gut 700 Programme samt bilateraler Vereinbarungen braucht.

Solche Programme mögen vielfach trivial sein, vor allem im DNA-Bereich, wo inzwischen ein gemeinsamer Satz von Merkmalen definiert ist, aber Arbeit ist es doch, und Verhandlungen braucht es auch.

So läuft der automatische Teil von Prüm nur schleppend an. Ende 2009 sagt die Bundesregierung (Drucksache 16/14150), DNA-Daten würden im Augenblick mit fünf Staaten, Fingerabdruck-Daten nur mit Österreich ausgetauscht. Fünf Staaten könnten in der Kfz-Datenbank ZEVIS recherchieren, während keine ausländischen Kfz-Datenbanken zugänglich seien. Es mag sein, dass die Regierung da nicht ganz richtig informiert ist, denn die Angaben widersprechen mehr oder weniger simultanen Angaben der österreichischen Ratsdelegation (Mitteilung 16623/09), und im Kfz-Bereich gibt es schon längst das EUCARIS-Verfahren, aber es bleibt doch bei Unzufriedenheit und Hader.

Die entstanden auch, weil einige Polizeien recht routinemäßig Prüm-Anfragen rausschickten. Das überflutete die Systeme kleiner Staaten, deren Big Brothers auf ihre eigene kleine Untertanenschaft ausgerichtet sind und nicht wie das BKA auf zehntausende von Anfragen pro Tag. Das führte schon 2008 zu intensiven Appellen des Rates an die Polizeien, doch auch mal an die Kleinen zu denken. Inzwischen sind die Appelle entscheidener geworden, und es gibt eine riesige Matrix, aus der abzulesen ist, wie viele Abfragen wer aus welchen Ländern zu beantworten bereit ist. Die Größenordnungen liegen dabei zwischen fünf und hundert pro Tag, Kategorie und Land.

Bei all dem sollte nicht vergessen werden, dass wie üblich die Ergebnisse bei den unter Verweis auf Terror, Mord und Vergewaltigung eingerichteten Verfahren weit überwiegend Trivialkriminalität betreffen. Von den 5000 Treffern, die die BRD bis September 2009 im DNA-Bereich aus dem Ausland bekommen haben, betrafen 4800 irgendwas wie Diebstahl oder Widerstand gegen Vollstreckungsbeamte. Um Missverständnisse zu vermeiden: Das ist nicht der primäre Defekt, schon gar nicht aus politischer Sicht, denn die im Politbereich üblichen 129a-Verfahren rechtfertigen so oder so *immer* die weitestgehenden Grundrechtsverletzungen. Nein, bemerkenswert ist nur wieder die Chutzpe der Zierckes, Pofallas und Wiefelsputze beim Zermenscheln von Einwänden („Man muss auch mal an die Opfer denken“) im Angesicht solcher Zahlen.

Europol

Im Geiste der politischen Väter von Europol ist die europäische Semigeheimpolizei recht analog zum BKA konstruiert: Wo das BKA mal für länderübergreifende Kriminalität hätte zuständig sein sollen, war Europol für ihre staatenübergreifende Schwester gedacht. Beide sind inzwischen zu begeisterten Computerspielern geworden, Europol sieht sich gar selbst primär als „Information Broker“.

Das BKA teilt sein INPOL auf in Verbund-, Zentral- und Amtdateien; erstere werden primär von den Landespolizeien gefüttert und auch von ihnen abgefragt, während die anderen vom BKA gefüllt werden und dann von den Ländern (Zentraldateien) oder nur vom BKA und seinen Freunden (Amtsdateien) abgefragt werden. Ähnlich hat Europol eine Verbunddatei, die dort Europol-IS heißt und analog zum Kriminalaktennachweis des BKA angelegt ist, und Amtsdateien, die dort weniger miefig als Analysis Work Files (AWFs) gehandelt werden.

Die Mitgliedspolizeien sollen in Europol-IS Angaben zu Personen und Straftaten samt Hinweisen auf die aktenführenden Stellen speichern, wenn „bestimmte schwerwiegende Tatsachen“ auf Relevanz für die Themen von Europol hinweisen, um dann Übereinstimmungen über Ländergrenzen festzustellen. 140 solcher „Hits“ gab laut Europol im Jahr 2008, und niemand weiß, ob irgendwas draus geworden ist.

Europol-IS hätte im Jahr 2006 automatisch Daten von allen Mitgliedsstaaten erhalten sollen, aber wirklich geklappt hat das nur bei der BRD (Überraschung!) und den Niederlanden. Der automatische Datenaustausch funktioniert bis heute nicht mit allen Mitgliedsstaaten. Dennoch hat sich in den letzten Jahren Europol-IS von einer Lachnummer zu einem -- wenn auch seichten -- Datengrab entwickelt. Der letzte verfügbare Jahresbericht für 2008 gibt an, die Datenbank habe 90000 „Objekte“ enthalten (zum Vergleich: der KAN des BKA ist mit über 3.5 Millionen dabei). Verglichen mit den 35000 Objekten des Vorjahres deutet sich aber doch eine gewisse Reifung des Systems an.

Für den Fall, dass jemand inzwischen den Überblick verloren hat: Europol-IS speichert im Gegensatz zu SIS Verdächtigungen und Verurteilungen, während SIS Ausschreibungen hält, d.h. konkrete Wünsche

zum Verfahren mit Gespeicherten. Bei Prüm wiederum geht es meist um die Übertragung bestimmter Merkmale zwecks „Match oder nicht Match“, ohne dass am anderen Ende Datensätze entstehen. Es wäre interessant, herauszubekommen, wie viele Freunde und Helfer dies durchschauen.

Analyse und Arbeit

Der Obergrusel bei Europol sind aber die Analysedateien (AWFs). Darin darf Europol von „Arbeitgeber“ bis „zugehörige Videos“ alles speichern, was gerade im Belieben der Beamten ist. Die generelle Haltung hier spiegelt sich recht nett Artikel 5, Absatz 2 der Durchführungsbestimmungen zu den AWFs wieder:

Der Direktor legt [...] fest, ob Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben [...] in die Arbeitsdatei zu Analyse Zwecken aufgenommen werden dürfen und warum diese Daten als unbedingt erforderlich für die entsprechende Arbeitsdatei zu Analyse Zwecken angesehen werden.

Der Direktor also. Im Umkehrschluss ergibt sich die Europol-Praxis, alle anderen Daten zu speichern, egal, ob das „unbedingt erforderlich“ ist oder nicht. Das also bleibt übrig von den Datenschutzprinzipien Datensparsamkeit („nichts speichern, was nicht klar zur Erfüllung eines verhältnismäßigen Zwecks erforderlich ist“) und Zweckbindung („dieser Zweck kann sich nicht mittendrin ändern“), draußen in der vom Nordseewind gepeitschten Realität von Den Haag.

Glücklicherweise kümmert sich Europol derzeit aber offenbar nicht sehr intensiv um Politgruppen. Die rund 20 AWFs beschäftigen sich mit Themen wie Drogenhandel, Rockergruppen, Islamisten, der Russenmafia oder Geldfälschung, besonders aber natürlich mit „Menschenhandel“ a.k.a. Migrationskontrolle; selbst die AWFs, die unter „Terror“ laufen, haben einen deutlichen Hautgout in dieser Richtung.

Glücklich ist dieses gegenwärtige Desinteresse auch, weil sich mit einer Analysedatei „Gewalttäter links“

für die deutschen Polizeien ein wunderbares Zwischenlager für Daten eröffnen würde, die sie in der BRD nur illegal speichern können. Die externe Lagerung erlaubt dazu noch eine Flucht vor der verfluchten Auskunftspflicht im Inland, denn Europol-Daten sind für die Untertanen praktisch unzugänglich.

Zwar kennt auch die Europol-Übereinkunft ein Auskunftsrecht der Opfer, doch darf eine Auskunft unterbleiben, wenn „Rechte und Freiheiten Dritter“ betroffen wären (in deutschen Regelungen dieser Art muss schon mal mindestens die Obrigkeit bedroht sein, damit das läuft), was sich immer konstruieren lässt. *Wirklich* unfassbar allerdings ist, dass von der Auskunft „unmittelbar betroffene Mitgliedsstaaten“ Einspruch erheben können und Europol daraufhin schon die *Tatsache der Speicherung* vor dem/der Anfragenden geheimhalten muss.

Bei derart haarsträubenden Verhältnissen kann nur noch auf Zynismus zurückgeführt werden, dass Europol selbst die Datenschutzstandards von Drittländern beurteilt, wenn diese auf die Daten in den AWFs zugreifen wollen. Glücklicherweise ist diese eklatante Bock-zum-Gärtner-Nummer letztlich irrelevant, denn, so der EU-Rechtsakt 2004/C 2/1, kann Europol Daten in beliebig korrupte Staaten verschieben, wenn „der Direktor von EUROPOL es für absolut notwendig hält“.

Am Rande noch: die Software, die die AWFs realisiert, wird von der Berliner Firma *rola security solutions* geschrieben. Diese wurde, *newsflash*, vor ein paar Monaten Ziel einer direkten Aktion mit Farbe und Steinen. Angesichts der überragenden Bedeutung ihrer Produkte für Freiheit, Demokratie und Rechtsstaatlichkeit, könnte sich jetzt die Bundesanwaltschaft für Menschen interessieren, die sich mit der Spitzentechnologie aus der Hauptstadt beschäftigen. Ob sie das tut, bleibt unklar. Zwar sind ein paar Google-Suchen nach *rola* von Unvorsichtigen, die kein *refcontrol*¹ oder ähnliches verwenden, auf *datenschmutz.de* eingetroffen, aber weils bei uns anonym zugeht (wir speichern natürlich keine IPs), haben wir keine Hinweise auf eventuelle offizielle Funktionen.

Murks ist unser Freund

Auch bei diesen Projekten bleibt festzuhalten, dass sich die Obrigkeiten fast beliebige Entwicklungsmöglichkeiten der Überwachungsgesellschaft in ihre Geset-

ze geschrieben haben. Angesichts des Offenbarungseids allen Gesäusels von Menschenrechten ist das, was uns bisher vor der Totalerfassung gerettet hat, das Misstrauen der Obrigkeiten untereinander und die wohlbekannten EDV-Katastrophen im Selbstbedienungsbereich der „Sicherheits“-Industrie.

Zur Illustration sei aus dem Europol-Jahresbericht 2008 zitiert, in dem die EDV-Abteilung sagt, irgendwas sei gemacht worden, um „den Einfluss der Stakeholder zu vergrößern und die Rolle des Produktmanagements in den nationalen Stellen der Mitgliedsstaaten zu etablieren“ (unsere Übersetzung). Dilbert-KennerInnen wissen, was solche Sätze heißen: „Wegen des Fehlens einer Testplattform und Ressourcenmangels wurden bislang keine Tests durchgeführt“ (Jahresbericht 2003, unsere Übersetzung).

Auf Dauer wird uns das nicht retten. VIS etwa, eine EU-Datenbank, die 20 Millionen Fingerabdrücke pro Jahr (!) sammeln soll (nämlich von allen, die EU-Visa beantragen), begann 2002, und es sah lange so aus, als würde es nichts werden. Nun allerdings scheint eine Inbetriebnahme im Dezember 2010 doch sehr wahrscheinlich. Wer fast unbegrenzte Geldmittel und wilde Entschlossenheit vereint, kriegt seine Überwachungsprojekte am Ende doch implementiert.

Die Entschlossenheit haben die EU-InnenministerInnen mit ihrem neuen Stockholm-Programm wieder dokumentiert. Tony Bunyan, Herausgeber des Bürgerrechte-Newsletters *Stawatch*, sieht als dessen größte Neuerung das „erklärte Ziel, die Überwachungsgesellschaft und den Datenbankstaat“ zu schaffen. In der im letzten Dezember verabschiedeten Fassung des Fünfjahresplans sorgt jede Menge Sprachkosmetik dafür, dass dieses Ziel nicht mehr ganz so deutlich erkennbar ist wie in den durchgesickerten Entwürfen, auf die Bunyan sich bezog. Doch ändert Schminke selten das Denken.

Auf der Stockholmer Wunschliste stehen ein Entry-Exit-System, quasi eine Vorratsdatenspeicherung für *alle* Grenzübertritte (incl. von EU-BürgerInnen), ECRIS, eine EU-Fassung des Bundeszentralregisters (da kommen die Führungszeugnisse her) und EPRIS, angelegt wohl als Europol-IS „für alles“, also ggf. bis runter zum Ladendiebstahl.

Die Erfahrungen mit SIS, Prüm und Europol lassen erwarten, dass diese Geisterbahn bis 2020 etwa zur

Hälfte eingerichtet sein wird. Für Nervenkitzel satt reicht auch das schon.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

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

¹Wer nicht will, dass (u.a.) alle Webseiten, auf die ihr von Google aus kommt, eure Suchwörter mitkriegen, solltet ihr eurem Firefox die Erweiterung RefControl (unter Erweiterungen suchen) gönnen. Browserübergreifend gibts es eine vergleichbare Funktionalität mit Programmen wie privoxy (<http://www.privoxy.org>), doch fällt dabei etwas Aufwand für Installation und Konfiguration an.