Daten und Menschen unterwegs

Zugriffe der Polizei auf Daten Dritter, Teil 1

Mit am Anfang der Entwicklung polizeilicher EDV standen die Rasterfahndungen der 1970er Jahre, in denen Staatsfeinde durch eine Kombination von „kriminologischem Instinkt“ mit allerlei Daten etwa von Meldeämtern und E-Werken gefunden werden sollten. Erste Erfolge dabei begründeten nicht nur den Mythos der allwissenden Polizei, sie schufen auch einen nicht stillbaren Appetit des Staatsapparats auf das, was auf den Festplatten privater oder öffentlicher Stellen liegt. Folgerichtig werden seither regelmäßig Gesetze geschrieben, die den Polizeien direkten oder jedenfalls ausnahmsweisen Zugriff auf viele Datenbestände genehmigen. Einige Beispiele dafür wollen wir in einer kleinen Reihe von Artikeln vorstellen.

Jeder Diskussion polizeilicher Zugriffe auf Datenbestände Dritter muss vorausgeschickt werden, dass im Strafverfahren ohnehin kaum Daten sicher sind. Die Vorschriften zu Sicherstellung und Beschlagnahme der Strafprozessordnung werden nämlich auch für „immaterielle Güter“ angewandt. Eine Sicherstellung bedarf dabei der Zustimmung des „Eigentümers“, aber in der Regel keiner Überprüfung durch Gerichte, eine Beschlagnahme setzt Letztere normalerweise voraus – was in der Praxis kein ernsthaftes Hindernis darstelt –, kann aber auch gegen den Willen der Eigentümer erfolgen. Noch häufiger schließlich bedient sich die Polizei privater EDV einfach auf dem Wege der freundlichen Nachfrage. Offizielle Zahlen zum Umfang solcher Aktivitäten gibt es aber nicht.

Daten sicher stellen

Es ist davon auszugehen, dass wenige Einrichtungen, die alltäglich mit euren Daten umgehen – sagen wir, Webseitenbetreiber – freundlichen Bitten um Sicherstellung der einen oder anderen Datei Widerstand entgegensetzen würden, soweit nicht Sorgen um „Geschäftsgeheimnisse“ oder steuerrelevante Erkenntnisse anstehen. Google allerdings gibt an, in der zweiten Jahreshälfte immerhin 26% der Anfragen aus der BRD nicht erfüllt zu haben, was die Firma viel strenger machen würde als deutsche Gerichte, die praktisch keine Durchsuchungs- oder Überwachungsanordnungen kassieren; dies wäre um so erstaunlicher, als der Behördenzugriff auf die meisten Daten, die Google so herausrücken dürfte – Telekommunikations-Bestandsdaten nämlich – , in §14 Telemediengesetz formell und ausgesprochen großzügig geregelt ist.

Ein recht bunter Versuch der Nutzbarmachung privater Daten kam im letzten Jahr aus Sachsen. Die dortige Polizei versuchte im Zusammenhang mit den 2011er Blockaden in Dresden brieflich, Busunternehmen, die Menschen zu den Aktionen hatten fahren lassen, zu umfangreichen Auskünften über Kontaktpersonen, FahrerInnen, Pausen, Ziel usf. zu bewegen. Ein anderer Coup des dortigen LKA war die Nutzung von Kassendaten von OBI-Baumärkten zur Aufklärung von Brandanschlägen auf Militäreinrichtungen im Jahr 2009. Offenbar war der Plan, Ort und Zeit des Kaufs bestimmter Artikel mit bei Telefonunternehmen gespeicherten Mobilfunk-Standortdaten zu kombinieren; wie viel davon umgesetzt wurde, ist derzeit nicht ganz klar, die Ermittlungen sind jedenfalls nicht recht vorangekommen.

Verrechtlichter Zugriff

Indes gibt es umfangreiche Datenbestände in Händen Dritter, auf die die Polizei direkten Zugriff hat, vielfach auch schon vor eventuellen Strafverfahren. Zu diesen gehören beispielsweise Daten der Meldeämter und des Kraftfahrtbundesamts, die Stammdaten der Banken (also nicht die konkreten Überweisungsdaten), das Ausländerzentralregister oder auch

bei den Telekommunikationsunternehmen gespeicherte Daten. Teilweise sind Unternehmen verpflichtet, bestimmte Schnittstellen bereitzustellen. Bei den Banken ist etwa vorgeschrieben, dass allerlei Behörden einen bestimmten Satz von Daten ohne Kenntnis der Bank selbst durchsuchen können müssen.

Besonders undurchsichtig werden die Besitz- und Austauschverhältnisse persönlicher Daten dort, wo kommerzielle Angebote und hoheitliche Funktionen auf engem Raum zusammenkommen. Ein schönes Beispiel sind hier Flughäfen. Dort gibt es neben unzähligen Videokameras Grenzkontrollen, das absurde Theater der Sicherheitskontrollen, den Gepäckcheck, die Bordkartenprüfung, den Zoll und martialisch bewaffnete Streifen. Pop Quiz: was davon tun Beamte (für Extrapunkte: welche davon dürfen euch erschießen?), was öffentliche Angestelle, und was Angestellte von Flughafen oder Fluggesellschaft?

In diesem Geflecht werden mehrfach persönliche Daten erfasst und weitergegeben. Zunächst ist da ein Verfahren namens Advance Passenger Information oder API. Betroffen sind dabei die hoheitlichen Daten, die maschinenlesbar in Pass oder Personalausweis stehen, verknüpft mit Flugnummer und Route. Früher wurden solche Daten erst bei der Grenzkontrolle bei der Einreise vom Zielland erfasst und mit Datenbanken dort abgeglichen. Nach Nineeleven wollten die USA dafür mehr Zeit haben und forderten sie „im Voraus“ (deshalb „advance“). Der Zeitgewinn dürfte vor allem den Geheimdiensten dienen; schlagen deren Datenbanken an, wollen die Schlapphüte Zeit haben, erstmal nachzudenken, ob sie den anderen Behörden ihre tollen „Erkenntnisse“ mitteilen wollen.

Im Kielwasser der Madrider Anschläge vom 11.3.2004 hat sich auch die EU eine Rechtsgrundlage für API-Verfahren gegeben. In der BRD etwa gehen solche Informationen, wo überhaupt übertragen, an die Bundespolizei. Diese kann sie einen Tag lang auf ihre Tauglichkeit für Migrationskontrolle oder Verbrechensbekämpfung prüfen, insbesondere natürlich durch Abgleich mit anderen Datenbeständen. Finden sich keine Gründe fürs Weiterspeichern, müssen sie dann gelöscht werden. API-Daten sollen in der EU nur fließen, wenn eine Schengen-Außengrenze übertreten wurde (auch wenn jedenfalls Spanien offenbar API für Reisende mindestens aus dem UK haben wollte).

Der geringe Zeitvorteil von API und im Vergleich zu selbst erhobenen Passdaten restriktive Bestimmungen zum Datenschutz sorgen dafür, dass nach Auskunft der EU-Kommission API „nur von wenigen Mitgliedstaaten angewandt“ wird. Dies wirft natürlich ein Schlaglicht auf Wert von Phrasen wie „Vakuum vermeiden“ und „grundlegende Bedeutung“, mit denen die API mandatierende Ratsrichtlinie wie üblich gespickt ist.

PNR

Erheblich reizvoller ist eine andere Kategorie von Daten, deren konsequente Nutzung ebenfalls auf den Korridoren des US-Department of Homeland Security vorangetrieben wurde: Die Passenger Name Records oder PNR. Dabei handelt es sich zunächst einmal um alles, was die Fluglinie über ihre Passagiere weiß. Als Industriestandard für den PNR hat sich in etwa Folgendes durchgesetzt:

- Buchungscode (wird bei der Buchung vergeben und identifiziert den PNR eindeutig), buchendes Reisebüro
- Datum von Reservierung sowie Ausgabe des Flugtickets
- Passagiernamen in der Fassung der Fluggesellschaft, ggf. weitere Namen von Mitreisenden, Reisestatus (z.B. Buchungsbestätigungen, Check-In)
- API-Daten (wo verfügbar; da sie maschinell generiert sind, taugen sie besser zur Verknüpfung mit anderen Daten)
- ggf. Vielfliegerstatus, Rabatte, Infos zu Buchungsteilungen
- Alle verfügbaren Kontaktinformationen
- Alle verfügbaren Rechnungs- und Zahlungsinformationen
- Reiseablauf, Ticket-Informationen (z.B. Flugscheinnummer, One-Way,...), besondere Bedürfnisse (von Fahrradmitnahme über koscheres Essen bis zur Notwendigkeit von Begleitpersonen ist da alles drin)
- Alle Informationen über das aufgegebene Gepäck, Sitzplatznummer

- Änderungsgeschichte des kompletten Datensatzes

Im Vergleich zum mageren API-Datensatz finden sich hier natürlich Delikatessen. Wer bar bezahlt, kein Schweinefleisch will und trotz weiter Reise kein Gepäck eingecheckt hat, darf sich auf eine unangenehme Einreise einstellen. Wenn diese Sorte von Daten zumal über Jahre (derzeit in den USA deren 15) hinweg aggregiert werden kann, fallen Weihnachten und Ostern für Geheimdienste wie ProfilerInnen mal wieder zusammen.

PNR-Daten seien „unique in their nature and their use“, fasst die EU-Kommission die Feierlaune in ihrem „global approach“ zu PNR-Daten zusammen. Und sie ist recht ehrlich, wenn sie erklärt, PNR-Daten sollten „re-active“, „real-time“ und „pro-active“ genutzt werden. Re-active ist die Nutzung der Daten zur Aufklärung von Verbrechen, während real-time und pro-active die Identifikation unerwünschter Personen bzw. unerwünschten Verhaltens aufgrund von Profiling bezeichnet sowie die Ableitung von Kriterien dafür: „prevent a crime, survey or arrest persons before a crime has been committed“ schreibt die EU-Kommission: Menschen verhaften, bevor sie Verbrechen begehen.

Phantasien über Minority Report kamen also ganz zu recht auf, als die USA kurz nach Nineeleven anfingen, PNRs zu erfassen, zunächst vermutlich direkt durch Zugriff auf die großen Reservierungssysteme, die von Firmen wie Sabre auf Rechnern in den USA für Fluggesellschaften in aller Welt betrieben werden. Wo das nicht reichte, konnte mit der Drohung mit dem Entzug der Landerechte nachgeholfen werden.

An dieser Stelle fühlten sich die europäischen Partner der Waterboarder vom Department of Homeland Security doppelt herausgefordert. Einerseits gefiel ihnen nicht, dass die USA so unter Umständen mehr Informationen über ihre Bürger hatten als sie selbst, andererseits wirkten die Möglichkeiten zur Gewinnung von „intelligence“, von wertvoller Information also, einfach zu verlockend. Ein PNR-System musste also auch für „uns“ her.

Der ersten Herausforderung wurde durch den Versuch einer Verrechtlichung der transatlantischen Datenverarbeitung begegnet, unter fast schon lächerlich wirkendem Verweis auf die dramatische Lage europäischer Fluggesellschaften, die von den USA zur Missachtung europäischer Datenschutzmaßstäbe gezwungen würden. Da die US-Seite die Daten ja schon hatte und die Kommission am Datenschutz allenfalls machtpolitisches Interesse zeigt, waren die resultierenden Vereinbarungen im Wesentlichen Kodifizierungen der Wünsche der US-Staatssicherheitsbehörden. Wie albern diese Vereinbarungen eigentlich sind, zeigte sich, als der Europäische Gerichtshof mal eine kassierte, das aber genau keine Konsequenzen hatte. Darüber hinaus standen die wesentlichen Details anfangs ohnehin nicht in den Verträgen, sondern wurden durch allerlei typischerweise geheimen Nebenabsprachen geregelt.

Ringen in der EU

Dementsprechend kritisch waren die Äußerungen von außerhalb der beteiligten Machtapparate. Durchaus lesenswert sind hier einige erstaunlich scharfe Stellungnahmen aus dem EU-Parlament. Dennoch verhandelte die EU-Kommission analoge Verträge mit Australien und Kanada, während Großbritannien ein eigenes PNR-System in Betrieb nahm. Das UK-System lief zunächst nur auf Stichprobenbasis und kam wohl erst in den letzten Jahren wirklich auf Touren. Inzwischen sind auch Staaten wie Saudi-Arabien, Japan und Südkorea schwer im PNR-Geschäft, innerhalb der EU haben die Regierungen von Frankreich, Dänemark, Belgien, Schweden und der Niederlande Gesetze abnicken oder gar schon Systeme zur PNR-Totalerfassung entwickeln lassen.

Womit sich für die EU das andere Problem – wir wollen sowas auch haben – verschärft stellt, denn PNR-Systeme leben von einer möglichst vollständigen Erfassung möglichst vieler Daten. Die verschiedenen EU-Stellen aber diskutieren nun schon fast ein volles Jahrzehnt. Leider wurde dabei erstaunlich wenig die Frage diskutiert, was für eine Sorte Staat überhaupt Kreditkartendaten, Telefonnummern und Sitzplatzpräferenzen von Reisenden über Jahrzehnte speichern und datenminen würde. Stattdessen ging es um Fragen wie: ein zentrales System oder viele nationale? Ist nur Terror der Zweck oder geht es auch um Verbrechen, Ordnungswidrigkeiten, ordinäre Grenzkontrollen? Sollen nur Flüge über die Schengengrenze hinweg erfasst werden, nur internationale Flüge, alle Flüge, oder auch noch Schiff- und Bahnfahrten? Fünfzehn Jahre oder fünfzehn Monate speichern? Wer darf Daten wann warum weitergeben?

Erfreulicherweise hat sich das EU-Parlament 2008 nicht auf dererlei Datenschutzbarock eingelassen und gesagt, es wolle überhaupt nicht über so einen Wahnsinn abstimmen. Geholfen hat das natürlich nicht viel: Völlig vorhersehbar steht die PNR-Verarbeitung wieder unter der Kategorie überlebenswichtig im Stockholm-Programm, dem aktuellen Fünfjahresplan des EU-Sicherheitssumpfes. Und so hat die Kommission im Feburar mal wieder einen Richtlinienentwurf zu EU-PNR vorgelegt.

In ihm ist vorgesehen, dass nur Flüge über Schengengrenzen hinweg erfasst werden, und zwar in jeweils eigenen nationalen Systemen (orwell-kompatibel „Passenger Information Units“ oder PIUs genannt), wobei Staaten aber kooperieren dürfen. Die Daten sollen explizit zum Data Mining verwendet werden, in der Tat ist Aufgabe der PIUs, Kriterien zur Vorhersage von Verbrechen zu erarbeiten. Das sattsam bekannte, aber nie definierte „serious crime“ (Gipfelproteste gehören jedenfalls dazu) soll auch bekämpft werden.

Die Speicherfrist auf EU-Ebene ist mit großzügigen fünf Jahren für Verhältnisse des menschenrechtsfreien Raums PNR-Verarbeitung noch eher im moderaten Bereich. Die Vorschrift, dass nach 30 Tagen Namen und Adressen relativ Unverdächtiger nur noch ein paar hochrangigen Beamten zugänglich sein sollen, ist indes erfahrungsgemäß praktisch wertlos. Hochrangige Beamte können nicht mit Rechnern umgehen, also werden sie ihre Zugriffsrechte streuen. Zudem sind solche Zugriffsbeschränkungen im geheimpolizeilichen Umfeld wertlos, weil sie genau dann fallen, wenn sie Personen schützen könnten.

Parallel zur eigenen Gesetzgebung verhandelt die Kommission derzeit neue PNR-Abkommen mit Australien und den USA. Die Empörungen des EU-Parlaments haben insofern geholfen, als die Verträge inzwischen mehr oder minder öffentlich sind und es sogar Versuche gibt, tatsächlich zu definieren, was „Terror“ eigentlich sei. Der aktuelle Vertragsentwurf mit Australien (Ratsdokument 10093/11) schlägt da z.B. vor die Schaffung eines „risk of damage to property“ um „a government or international organisation“ zu zwingen „to act or abstain from acting“. Es ist schwer, sich irgendeine politische Aktion vorzustellen, die von dieser Definition nicht erfasst würde.

Precrime

Bei den PNR-Diskussionen fällt immer wieder auf, wie wenig sich die Regierungen Mühe geben, Rechtsstaat zu spielen. In einem Bericht des britischen House of Lords von 2008 wird eine Mitarbeiterin des Innenministeriums zitiert, die als Fahndungserfolg der Monstrosität allen Ernstes ein paar Chinesen erwähnte, die mit gefälschten Papieren einreisen wollten. Und Zigarettenschmuggler. Dort wird auch angegeben, dass das UK-PNR-System bis dahin 38 Millionen PNRs verarbeitet und dabei 17000 Personen herausgefiltert hätte, von denen dann 1400 festgenommen worden seien. Einer von zwölf Belästigten sei damit „schuldig“ gewesen, so die Mitarbeiterin – so geht das im modernen Rechtsstaat, wer verhaftet wird, ist auch schuldig. Aus propagandahandwerklicher Sicht ähnlich enttäuschend hat für die BRD Innenminister Friedrich erklärt, die „Düsseldorfer Zelle“ – drei Leute, die Grillanzünder, Zitronensäure und Wasserstoffperoxyd gekauft haben sollen – hätte ohne aus PNR-Daten stammenden „Erkenntnissen“ aus den USA nie „ausgehoben“ werden können.

Nun könnte mensch einwenden: Dann fliegt halt nicht. Das allerdings bereuen wir spätestens, wenn ohne Personalausweis auch keine Zugfahrt mehr geht. Widerstand gegen die Precrime-Politik tut also Not. Dabei stehen die Chancen, öffentliche Resonanz zu bekommen, in den nächsten Monaten nicht schlecht, angesichts relativ offen eingestandener Normenverschiebungen, einer klaren breiten Betroffenheit bereits vom Securityzirkus genervter Reisender und eines wohl noch für eine Weile laufende Gesetzgebungs- und Verhandlungsverfahrens, das jedenfalls auf den hinteren Seiten der Zeitungen auch ohne linksradikale Intervention Platz finden dürfte. Den Spin dieser Nachrichten sollten wir nicht dem BKA überlassen.

Datenschutzgruppe der Roten Hilfe Heidelberg

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

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