Humanistische Union

Datenschutz-Index für Sicherheitsdatenbanken

aus: vorgänge Nr. 206/207 (Heft 2-3/2014), S. 152-162

(Red.)Um eine staatliche oder private Datenbank aus Datenschutzsicht angemessen bewerten zu können, müssen viele Dinge berücksichtigt werden. Dazu zählen u.a. die rechtlichen Rahmenbedingungen, technische Sicherheitsstandards, faktische Arbeitsabläufe. Entsprechend schwierig ist deshalb die bürgerrechtliche Bewertung einer Datenbank in einfachen Worten, die für Laien verständlich, übersichtlich und dennoch präzise ist. Für eine schnell zu erfassende Bewertung solcher Datenbanken könnte ein Datenschutz-Index helfen. Michael Kuhn stellt ein mögliches Modell eines solchen Indexes vor.

Die Anzahl staatlicher Datenbanken ist heute kaum mehr zu überschauen. So existierten etwa im Jahr 2011 allein für die polizeiliche Gefahrenabwehr und Prävention 69 bundesweite Datenbanken beim Bundeskriminalamt (BKA), der Bundespolizei und dem Zollkriminalamt. Diese Datenbanken enthielten 15.694.595 Datensätze, wie eine parlamentarische Anfrage der Linken (BT-Drs. 71/7160) ergab. Das lässt erahnen, welche Datenmassen bei staatlichen Stellen vorhanden sind, wenn man neben dem Bund auch die Länderebene oder die zahlreichen anderen behördlichen Tätigkeitsbereiche in den Blick nimmt. Selbst wenn diese Informationen alle zugänglich wären – sich einen schnellen Überblick über staatliche Datensammlungen zu verschaffen und ihr Gefährdungspotential für die Bürgerrechte zu erkennen, ist kaum zu leisten. Ausgehend von den Ergebnissen des Projekts „Staatliche Datensammlung – Sind Bürger_innen gefährdet?“, an dem sich die Humanistische Union in den letzten beiden Jahren beteiligte, möchte ich die Möglichkeiten und Grenzen eines Datenschutz-Indexes diskutieren, mit dem staatliche Datenbanken systematisch bewertet werden können.

Das Projekt „Staatliche Datensammlung – Sind Bürger gefährdet?

Die Schwierigkeiten, die es bereiten kann, aus der Vielzahl staatlicher Datenbanken die besonders problematischen und diskussionswürdigen herauszufiltern, wurden besonders deutlich bei der Durchführung des Projektes „Staatliche Datensammlung – Sind Bürger gefährdet?“ (nachfolgend „Projekt“).(1) Grundidee des Projektes war es, staatliche Datenbanken verschiedener Bereiche in einer Reihe europäischer Länder zu vergleichen. Die Ergebnisse des Vergleichs sollten in leicht verständlichem, übersichtlichem Informationsmaterial zusammengefasst werden. Dazu zählten ein Online-Quiz, ein Datenschutzpass und ein übersichtliches Ranking („Hitparade“) der untersuchten Länder, u.a. Deutschland, Großbritannien, Österreich, Frankreich, Portugal, Spanien, Ungarn, Polen, Tschechien, Luxemburg und Griechenland.

Bereits die Suche nach einer geeigneten Methode für den Vergleich der Datenbanken gestaltete sich als schwierig. Die Projektteilnehmer_innen einigten sich darauf, zunächst Datenbanken in jedem Feld nach ihrer Gefährlichkeit oder besonderen Relevanz in der öffentlichen Diskussion herauszusuchen und diese Einschätzung anhand eines gemeinsam entwickelten Fragebogens zu erklären. Die Fragebögen waren die

Grundlage für die gemeinsam erstellte vergleichende Analyse.

Allerdings war das Projekt auf die Erstellung von knappem und verständlichem Informationsmaterial für Bürger_innen ausgerichtet, das auch in mehreren europäischen Ländern funktionieren sollte. Die daraus folgenden Probleme, die umfangreichen Informationen und Wertungen nachvollziehbar und sinnvoll zu verdichten, zeigten sich besonders an der „Hitparade“. Das ambitionierte Ziel bestand darin, auf einer Druckseite die untersuchten Dateien in den verschiedenen Ländern knapp und übersichtlich nach ihrer „Gefährlichkeit“ in einem Datenschutzranking von „sehr gut“ bis „sehr schlecht“ darzustellen. Dazu wurden die Datenbanken anhand der Fragebögen in den Dimensionen „Gefährlichkeit“, „Transparenz“, „Rechtsschutzmöglichkeiten“ und „Einfluss der Datenschutzbehörden“ bewertet. Die dabei vergebenen Noten waren für die anderen Projektteilnehmer_innen aber kaum nachvollziehbar und die Gesamtergebnisse am Ende teilweise unplausibel. Ein Grund dafür mag gewesen sein, dass Datenbanken im eigenen Land – über das man schließlich am besten informiert ist – negativer bewertet werden als die ausländischen Datenbanken, die man nur aufgrund der Recherchen und der knappen Fragebögen kennt. Zudem waren die genannten Bewertungskriterien ohne weitere Erläuterung keineswegs selbsterklärend, weshalb die Bewertungen am Ende sehr subjektiv ausfielen. Ist z.B. der Rechtsschutz nur schwer, wenn falsche oder rechtswidrige Einträge schwer zu korrigieren bzw. löschen sind, oder bereits dann, wenn die Betroffenen nie oder nur in Ausnahmefällen über ihre Speicherung benachrichtigt werden (was i.d.R. die Voraussetzung für die Wahrnehmung des Rechtsschutzinteresses ist)?

Sinn eines Datenschutzindexes

Trotz der dargestellten Probleme beim datenschutzrechtlichen Bewerten und Vergleichen von Datenbanken stellt sich die Frage, ob die Grundidee einer knappen und aussagekräftigen Wertung von Datenbanken nicht doch sinnvoll ist und für die Arbeit einer Bürgerrechtsorganisation fruchtbar gemacht werden kann. Der Mehrwert eines solchen Verfahrens bestünde in einem konzentrierten Überblick über bestehende Datenbanken, mit dem Interessierte eine ihnen unbekannte Datenbank schnell beurteilen und die besonders problematischen Aspekte einer Datenbank schnell erfassen können. Damit geht ein Datenschutzindex in eine ähnliche Richtung wie das „Datenschutzgütesiegel“, das die Stiftung Datenschutz für den privaten Bereich erarbeiten soll. Im Gegensatz zu Verbraucher_innen haben Bürger_innen, die sich mit staatlichen Datenbanken beschäftigen, natürlich nicht die Möglichkeit, Produkte ohne Gütesiegel bzw. mit einer schlechten Wertung einfach zu meiden. Dennoch ist es möglich, mit Hilfe eines Datenschutzindexes ein besseres Bewusstsein für die Probleme staatlicher Datensammlungen zu schaffen und so das Interesse von Bürger_innen an der Wahrnehmung ihrer Auskunfts- und Beschwerderechte zu verbessern. Ein transparenter Datenschutzindex könnte an Initiativen wie „Reclaim your data“ anknüpfen. Eine griffige Bewertung von Datenbanken anhand einer Note, die evtl. mit Farben oder Symbolen untermalt wird (etwa wie das vieldiskutierte Wertungssystem der „Lebensmittelampel“) hätte zudem einen hohen Wiedererkennungswert und könnte eine Art Markenzeichen für den Datenschutz werden. Da die datenschutzrechtliche Debatte häufig um private Akteure wie Facebook oder Google kreist, könnte der Datenschutzindex dazu beitragen, Bürger_innen bewusst zu machen, dass auch der Staat in kaum überschaubarem Ausmaß persönliche Daten speichert und verknüpft.

Grundsätzliche Probleme und Grenzen eines Datenschutzindexes

Das Projekt „Staatliche Datensammlung“ hat die grundsätzlichen Schwierigkeiten bei der Erarbeitung eines Datenschutzindexes deutlich gemacht. Aus den Erfahrungen kann man folgern, dass auf eine datenschutzrechtliche Gesamtbewertung ganzer Politikfelder oder ganzer Länder aufgrund des Umfangs und

der Komplexität des Themas besser verzichtet werden sollte. Die Ergebnisse wären entweder sehr vage oder aufgrund individueller Besonderheiten ohne eingehende Hintergrundinformationen kaum verständlich; vor allem, wenn man eine knappe rechtsvergleichende Bewertung darstellen möchte. Das lässt sich an den teilweise ganz unterschiedlichen nationalen Befindlichkeiten verdeutlichen. So wird etwa das Melderegister in Deutschland kaum grundsätzlich problematisiert, während die Einführung eines vergleichbaren Registers in Großbritannien nach einer großen öffentlichen Debatte gestoppt wurde. Umgekehrt wäre eine zentrale Schülerdatei voll sensibler Daten, wie sie in Großbritannien existiert und erstaunlich wenig diskutiert wird, in Deutschland politisch und rechtlich undenkbar. Sicherlich können auch breit angelegte Vergleiche zu informativen Ergebnissen führen, die als Diskussionsgrundlage nutzbar sind. Das zeigen nicht zuletzt der Privacy Index oder der Surveillance Monitor von Privacy International.

Verengt man den Fokus dagegen auf die Bewertung einzelner nationaler Datenbanken, lässt sich jedoch ein Datenschutzindex präziser und zugleich handhabbarer gestalten. Dabei muss jedoch das methodische Vorgehen transparent gemacht werden. Eine einzelne Bewertung einer Datenbank allein ist aufgrund der vielfachen Ausgestaltungsmöglichkeiten von Datenbanksystemen, der darin gespeicherten Daten und ihrer Verwendungen kaum aussagekräftig. Die Aussagekraft der Bewertung beruht daher auf der Angabe der einzelnen untersuchten Kriterien und der Angabe, mit welcher Gewichtung diese in die Bewertung eingehen. Letztlich bleibt eine solche Bewertung von Datenbanken dennoch subjektiv, wird aber zumindest nachvollziehbar und in sich konsequent.

Folgerungen und Skizze eines möglichen Vorgehens

Ausgehend vom Projekt „Staatliche Datensammlung“ erfolgt die Analyse einer zu bewertenden Datenbank anhand eines einheitlichen Rasters, das in mehrere Kategorien unterteilt ist. Einige Kategorien sind rein informativ, wie etwa die Auflistung der nationalen und ggf. europäischen Rechtsgrundlagen, die zuständigen Behörden (für evtl. Auskunftsersuchen), das Datum der Errichtung, ggf. die Vorgeschichte der Datenbank, Stellungnahmen der Datenschutzbehörden oder zivilgesellschaftlicher Initiativen. Für die eigentliche Bewertung sind dagegen fünf Kategorien maßgeblich: Zweck, Inhalt, Datenzugriff, Datenverwaltung und Datenkontrolle. Nach diesen Kriterien wird die Datenbank bewertet, wobei sich die Schulnotenskala von 1 (sehr gut) bis 6 (ungenügend) anbietet.

Die Benotung sollte erläutert werden, da ein solches System nicht selbsterklärend ist. Als Grundlage der Benotung kann zunächst eine Sammlung kurzer Beispiele dienen, die Hinweise zur Gewichtung der einzelnen Kriterien gibt und möglichen Missverständnissen vorbeugt. Trotz der angestrebten Systematik sollte das Bewertungsschema aber offen gestaltet sein, um den Besonderheiten der individuellen Datenbank zu entsprechen. Das Bewertungsraster kann sich mit seiner Anwendung in der Praxis und den sich dort zeigenden Zweifelsfragen weiter entwickeln, wäre also kein starres Muster. In der genaueren Ausarbeitung wäre auch zu überlegen, ob die Bewertungskriterien und ihre Erläuterungen je nach dem Anwendungsbereich der Datenbank (z.B. Polizei, Gesundheitswesen, Bildung) variieren sollten und ob zwischen privat geführten Datenbanken – ob privat veranlasst oder auf staatlicher Anordnung beruhend – unterschieden werden soll. Die Aussagekraft der am Ende gebildeten Abschlussnote (Gesamturteil) würde dadurch erhöht, dass auch die Teilnoten der verschiedenen Bewertungskategorien ausgewiesen werden, um die verschiedenen Bewertungsdimensionen darzustellen. Es wäre ja vorstellbar, dass eine Datenbank, die hochsensible Daten enthält, in den anderen Aspekten vorbildlich ausgestaltet ist, was eine Gesamtnote nicht abbilden kann.

Unter Berücksichtigung dieser Einschränkungen schlage ich als Ausgangspunkt die folgenden Kategorien und exemplarischen Bewertungskriterien vor. Sie orientieren sich an der juristischen Prüfung der Rechtfertigung eines Grundrechtseingriffs, insbesondere der Verhältnismäßigkeitsprüfung, und greifen die

typischen Datenschutzprobleme staatlicher Datenbanken auf.

I) Zweck

1. Für welche (zulässigen) Zwecke werden die Daten erhoben?
2. Gibt es Zweifel an der Geeignetheit/Erforderlichkeit der Maßnahmen zur Zweckverfolgung ganz generell?
3. Gibt es Nachweise für die Geeignetheit/Erforderlichkeit der Maßnahmen mit Blick ganz generell auf den Zweck?
4. Bestehen Bedenken, dass tatsächlich hauptsächlich andere Zwecke verfolgt werden könnten? Wird das Zweckbindungsgebot eingehalten?
5. Besteht die konkrete Gefahr der Ausweitung auf weitere (Verwendungs-) Zwecke

II) Inhalt

Leitfragen: Ist das Ausmaß der gespeicherten Daten verhältnismäßig zur Zweckverfolgung? Genügen die Regelungen dem Bestimmtheitsgebot?

1. Welche Kategorien von personenbezogenen Daten werden erfasst? Sind diese bestimmt genug?
   a) Allgemeine Kategorien personenbezogener Daten:
   * Einzelangaben über persönliche Verhältnisse zur Identifizierung und Beschreibung des/der Betroffenen (z.B.: Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf, Ausbildungsstand, Erscheinungsbild, Leistungen, Arbeitsverhalten, Gesundheitszustand oder Überzeugungen)
   * Einzelangaben über sachliche Verhältnisse mit Art der Zuordnung zur Person (Name oder Nummer)
   b) Besondere Kategorien von Daten, zu denen es bereits Regelungen/Rechtsprechung gibt:
   * Stammdaten/Bestandsdaten (vgl. §§ 97, 111 TKG)
   * Verkehrsdaten (vgl. § 96 TKG)
   * Standortdaten (vgl. § 98 TKG)
   * Zugangsdaten (vgl. § 113 Abs.1 S. 2 TKG, 100j Abs. 1 S. 2 StPO)
2. Sind die erfassten Daten(-kategorien) sensibel?
   * Werden sensible Daten i.S.v. §§ 3 Abs. 9, 35 Abs. 2 S. 1 Nr. 2 BDSG erfasst?
   * Haben die Daten Diskriminierungspotenzial?
   * Kann durch die Aggregation von Daten auf sensible Daten geschlossen werden?
   * Gibt es bekannte Probleme mit den Datenkategorien, z.B. diskriminierende oder abschreckende Wirkungen?
3. Wie umfassend sind die erfassten Daten?
   * Wie groß ist der erfasste Personenkreis?
   * Beschreiben die Daten einzelne Personen, Beziehungen zwischen einzelnen Personen oder ganze Netzwerke?
   * Wie eng sind die Voraussetzungen zur Speicherung bzw. erfolgt die Speicherung sogar anlasslos?
   * Sind die Regelungen zum Inhalt klar umgrenzt? Besteht die Gefahr der (schleichenden) Ausweitung auf neue Daten?
   * Wie lange werden die Daten gespeichert?
4. Wie groß ist die Gefahr von Missbrauch/Profilbildung?

III) Datenzugriff und -verknüpfung

Leitfragen: Sind die Zugriffsregelungen verhältnismäßig zur Zweckverfolgung? Genügen die Regelungen dem Bestimmtheitsgebot?

1. Was sind die materiellen Voraussetzungen für den Zugriff?
2. Welche Stellen sind zugriffsberechtigt? Sind die Regelungen zum Zugriff klar?
3. Wird hinsichtlich des Zugriffs auf bestimmte Datenkategorien differenziert?
4. Gibt es Statistiken über die tatsächlichen Zugriffe/Abfragen? Wird die tatsächliche Verwendung der Datenbank evaluiert?
5. Wird exzessiv auf die Daten zugegriffen, ohne dass weniger belastende Maßnahmen zuerst ausgeschöpft werden (vgl. Funkzellenabfragen in Berlin)
6. Wird die Datenabfrage auf das für den Zweck Notwendige beschränkt?
7. Besteht die Gefahr der (schleichenden) Ausweitung der Zugriffbefugnisse?
8. Welche Verknüpfungen bestehen / könnten in Zukunft hergestellt werden (national/europaweit/international)?
9. Besteht die Möglichkeit einer Verwendung der Daten zu anderen Zwecken als denjenigen, die zur Speicherung berechtigt haben?

IV) Datenverwaltung

Leitfrage: Sind die Regelungen zur Datenverwaltung verhältnismäßig?

1. Wann werden die Daten gelöscht?
2. Wird die Datenbank zentral oder dezetral verwaltet?
3. Wird die Datenbank staatlich oder privat geführt?
4. Sind die Regelungen zur technischen Sicherheit der Daten ausreichend?
5. Werden die Daten bei der abrufenden Stelle nach Verwendung gelöscht?
6. Können diese Regeln effektiv kontrolliert werden?

V) Selbstschutz und Datenkontrolle

Leitfrage: Sind die Regelungen zur Datenkontrolle verhältnismäßig?

1. Wie transparent ist die Datenbank? Wird verdeckt gespeichert?
2. Welche Auskunfts-, Widerspruchs- und Berichtigungsrechte hat der/die Betroffene? Sind dieseeffektiv durchsetzbar?
3. Wird der/die Betroffene über die Erhebung/Nutzung seiner/ihrer Daten benachrichtigt? Gibt es Ausnahmevorschriften, und wenn ja: Bleibt damit die Benachrichtigung der Regelfall, oder wird sie zur Ausnahme?
4. Sind die Rechte der Datenschutzbehörden ausreichend?
5. Sind die Rechte der Datenschutzbehörden effektiv durchsetzbar?

In diesen fünf Kategorien wird jeweils eine Einzelnote vergeben. Das Raster sollte als Erläuterung zur Gesamtbewertung mitveröffentlicht werden und ist so auszufüllen, dass der/die Leser_in für die problematischen Eigenschaften der Datenbank sensibilisiert und über seine/ihre Rechte informiert wird. Die Fragebögen im Projekt „Staatliche Datensammlung“ waren im Vergleich oft zu detailliert und durch die umfassende Aufzählung von Rechtsnormen unübersichtlich. Das hier vorgeschlagene Bewertungsraster sollte dagegen nicht mit (rechts-)wissenschaftlichem, sondern mit informativem Anspruch ausgefüllt werden. Zur besseren Verständlichkeit könnte ein kürzerer Fließtext auf die bemerkenswerten positiven und negativen Punkte aufmerksam machen.

Bei der Gewichtung der einzelnen Kriterien ist zu beachten, dass die negative Benotung einer Datenbank von nur einem negativen Punkt in der jeweiligen Kategorie abhängen kann, wenn etwa der erfasste Personenkreis unverhältnismäßig weit ist. Wenn ein Defizit von großem Gewicht ist, sollte es auch auf die Gesamtbewertung durchschlagen. Diese Vereinfachung ist dem Vorgehen immanent und findet sich auch bei anderen Bewertungssystemen. Wird etwa ein elektronisches Gerät von der Stiftung Warentest untersucht, erhält es ggf. auch eine mangelhafte Gesamtnote, wenn nur der Stecker einen Fehler hat, der aber zu akuter Brandgefahr führt. Es gibt also Defizite, die nicht durch ansonsten gute Bewertungen ausgeglichen werden können.

Die Bewertung einer einzelnen Datenbank kann graphisch aufbereitet werden. Dafür bietet sich beispielsweise ein Ampelsystem an, das die Gesamtnote wiedergibt. Darüber hinaus sollten Kurzinformationen zu Namen, Zweck und Rechtsrahmen der Datenbank angeben werden. Weitere Symbole bieten sich an, die auf besondere Umstände hinweisen: etwa wenn eine Datenbank ganz oder zum Teil von Gerichten für gesetzes- bzw. verfassungswidrig erklärt wurde. Ein weiteres Zeichen könnte darauf aufmerksam machen, dass die Datenbank besonders gut beobachtet werden muss, da die Gefahr einer Verschlechterung etwa durch Ausweitung der Zugriffsrechte besonders groß ist. Schließlich wäre auch ein Symbol denkbar, das darauf hinweist, dass eine Datenbank bisher in der Öffentlichkeit nicht die kritische Aufmerksamkeit erfährt, die eigentlich angebracht wäre.

Beispiel: Die Bewertung der Antiterrordatei

Nach dem hier unterbreiteten Vorschlag wird nun als Beispiel die sogenannte Antiterrordatei bewertet. Das ausführliche Raster kann zusätzlich zugänglich gemacht werden. Dabei handelt es sich um eine gemeinsame Datenbank deutscher Geheimdienste, Polizei- und Sicherheitsbehörden, in der terrorverdächtige Personen, deren Unterstützer_innen und Kontaktpersonen sowie die von ihnen genutzten Einrichtungen gespeichert werden.

Aufgrund der Komplexität der Datei ist es aus Platzgründen nicht möglich, das Raster komplett auszuführen. Deshalb wird nur eine Kurzfassung zur Begründung der Einzelnote angegeben, um den Inhalt und die

Bedeutung der Kategorien zu veranschaulichen. Am Ende wird noch eine einfache graphische Darstellung vorgeschlagen.

I) Zweck – Note „3“

Zweck der Antiterrordatei ist die Bekämpfung des internationalen Terrorismus durch Ermöglichung von Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten.

Die Benotung des Zwecks an sich ist problematisch. In der juristischen Prüfung unterfällt er nur dem sehr groben Filter der Legitimität, d.h. das Ziel muss nach der Verfassung nur grundsätzlich zulässig sein. Im Rahmen des Bewertungsrasters sollten jedoch ggf. auch verfassungsrechtlich legitime Ziele abgestuft bewertet werden, etwa wenn – wie hier wegen der damit verbundenen Aufweichung des Trennungsgebotes zwischen Polizei und Nachrichtendiensten – bereits der Zweck an sich grundsätzlich umstritten oder besonders missbrauchsanfällig ist.

II) Inhalt – Note „5“

Die Kriterien für die Speicherung von Personen finden sich in § 2 ATDG. Die in der Antiterrordatei gespeicherten Personen müssen bereits von den beteiligten Behörden (den Polizeien und Geheimdiensten des Bundes und der Länder) erfasst sein. Im Wesentlichen werden u.a. Personen gespeichert, bei denen sich tatsächliche Anhaltspunkte dafür ergeben, dass sie einer terroristischen Vereinigung mit internationalem Bezug angehören, dass sie eine solche Vereinigung unterstützen, rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen, sowie Kontaktpersonen dieser Personen (d.h. die nicht nur flüchtig oder in zufälligem Kontakt stehen) und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind.

Die Regelungen zum Kreis der gespeicherten Personen wurden vom Bundesverfassungsgericht teilweise als unverhältnismäßig und verfassungswidrig eingestuft. Problematisch ist grundsätzlich bereits die Speicherung aufgrund von Verdachtsmomenten, die im Einzelfall unverhältnismäßig sein kann und daher stets verfassungskonformer Anwendung bedarf. Bei Unterstützern terroristischer Vereinigungen werden dagegen noch nicht einmal Verdachtsmomente erwartet, dass sie von den terroristischen Aktivitäten Kenntnis haben. Damit ist das Verhältnismäßigkeitsgebot verletzt.

Teilweise sind diese Regelungen zu unbestimmt. So bedarf der Begriff „rechtswidrige Gewalt“ einer einschränkenden Auslegung, da der strafrechtliche Gewaltbegriff sehr weit reicht. Gleiches gilt für das „vorsätzliche Hervorrufen“ von Gewalt vor dem Hintergrund, dass der strafrechtliche Vorsatzbegriff auch die bewusste Fahrlässigkeit umfasst. Zu weit ist schließlich auch das „Befürworten“ von Gewalt, da hier nur an den Verdacht einer inneren Haltung angeknüpft wird, den der/die Einzelne selbst durch völlig rechtstreues Verhalten nur begrenzt ausräumen kann. Die einschüchternde Wirkung dieses Tatbestandsmerkmals ist daher besonders groß. Auch die Regelung zu den „Kontaktpersonen“ ist zu weit und unverhältnismäßig. Auch wenn Personen mit „nur flüchtigem Kontakt“ ausgenommen sind, so erfasst die Norm doch praktisch das gesamte persönliche und private Lebensumfeld der Betroffenen. Vor diesem Hintergrund dürfen unwissende Kontaktpersonen zumindest nur verdeckt unter dem Eintrag der Hauptperson mit wenigen Grunddaten gespeichert werden.

Der Umfang der gespeicherten Daten ergibt sich aus § 3 ATDG. Für alle erfassten Personen werden Grunddaten zur Identifizierung gespeichert, für die meisten gespeicherten Personen – ausgenommen ahnungslose Kontaktpersonen – wird darüber hinaus eine ganze Reihe von erweiterten Grunddaten (wie Telekommunikationsanschlüsse, Bankverbindungen usw.) erfasst. Die erweiterten Daten können grundsätzlich nur zur verdeckten Recherche genutzt werden.

Der Umfang der gespeicherten Daten ist hochproblematisch. Bereits die zur Identifizierung dienenden Grunddaten lassen Rückschlüsse auf die Biographie der Person zu und erfassen sensible Daten (z.B. besondere körperliche Merkmale) sowie Merkmale mit hohem Diskriminierungspotential (z.B. Herkunft). Dies gilt erst recht für die Zusammenschau mit den erweiterten Grunddaten, die ein umfassendes Persönlichkeitsprofil erlauben. Die Speicherung dieser Daten kann nur mit Blick auf den gewichtigen Zweck der Terrorismusbekämpfung und der Tatsache gerechtfertigt werden, dass es sich um rechtmäßig erhobene Daten handelt, die nur zusammengetragen werden, bzw. bei denen die Möglichkeit zum Abruf nach dem jeweiligen Fachrecht der beteiligten Behörden geschaffen wird. Damit diese Vorschriften dem Bestimmtheitsgebot genügen, müssen die Datenkategorien in der Errichtungsanordnung gemäß § 12 Nr. 3 ATDG durch die Verwaltung zudem hinreichend konkretisiert werden. Das sogenannte Freitextfeld darf zudem nur zurückhaltend für punktuelle Erläuterungen zu anderen Daten verwendet und nicht als Blankoermächtigung verstanden werden.

III) Datenzugriff und -verknüpfung – Note „5“

Gegen das Bestimmtheitsgebot verstößt bereits, dass der Kreis der einspeisenden und abrufberechtigten Behörden im Gesetz nicht abschließend genannt ist und § 1 Abs. 2 ATDG die Öffnung für weitere Behörden durch Rechtsverordnung vorsieht.

§ 5 Abs. 1 Satz 1 und 2 ATDG geben den beteiligen Behörden einen unmittelbaren Zugriff auf die einfachen Grunddaten. Ein solcher Informationsaustausch im Vorfeld ist auch angesichts der großen Bedeutung der Terrorismusabwehr nur unter Einschränkungen verhältnismäßig. So darf es sich nur um Einzelabfragen handeln und keine systematische Rasterfahndung erfolgen. Zudem ist ein konkreter Ermittlungsanlass erforderlich. Eine Nutzung der Daten ist gem. § 6 Abs. 1 S. 1 nur zur Identifizierung der relevanten Personen und zur Vorbereitung von Einzelübermittlungsersuchen an die informationsführende Behörde erlaubt. Allerdings lässt das ATDG zu, dass Daten, die unter besonderen Voraussetzungen der Eingriffe in die Telekommunikationsfreiheit und die Unverletzlichkeit der Wohnung gewonnen wurden, ohne weitere Voraussetzungen in den Datenaustausch eingestellt werden und damit für Vorfeldermittlungen genutzt werden können, für die sie nicht erhoben werden durften. Diese Zweckentfremdung ist verfassungswidrig.

In Bezug auf die erweiterten Grunddaten ist grundsätzlich nur eine verdeckte Recherche möglich, d.h. Treffer werden nach einer Suche gemeldet, aber die erweiterten Grunddaten sind nicht bzw. erst auf Einzelersuchen nach Maßgabe des Fachrechts einsehbar. Unverhältnismäßig ist aber, dass bei Treffern in den erweiterten Grunddaten unabhängig vom Eilfall ein sofortiger Zugriff auf die einfachen Grunddaten eingeräumt wird. Ein solcher umfassender Einblick in die Daten ist zum eigentlichen Zweck der Abfrage – der Vorbereitung eines Informationsaustausches nach den fachrechtlichen Vorschriften – nicht erforderlich.

IV) Datenverwaltung – Note „3“

Das ATDG enthält selbst keine Vorschriften zur Datenverwaltung und verweist – auch in Bezug auf die Löschfristen – auf das Fachrecht. Zwar ist dieses Vorgehen wegen der Funktion der Datei zulässig,

erschwert aber die datenschutzrechtliche Kontrolle.

V) Selbstschutz und Datenkontrolle – Note „4“

Die Intransparenz der Antiterrordatei macht den Selbstschutz fast unmöglich. Das Gesetz selbst enthält nur wenige Regelungen zur Herstellung von Transparenz und individuellem Rechtsschutz. Im Wesentlichen begnügt es sich damit, die stark eingeschränkten Auskunftsrechte zu formulieren. Es bestehen weitreichende Ausnahmen von der Auskunftspflicht der Behörde, etwa wenn durch die Auskunft die Aufgabenwahrnehmung gefährdet wäre oder wenn zu befürchten sei, dass der Erkenntnisstand der Behörde ausgeforscht werden soll. Verdeckt gespeicherte Daten müssen nach § 10 Abs. 2 ATDG nicht einheitlich beim BKA, sondern von den einzelnen informationsführenden Behörden abgefragt werden. Dies lässt sich zwar damit rechtfertigen, dass das BKA selbst diese Daten nicht einsehen kann – erschwert angesichts von über 60 teilnehmenden Sicherheitsbehörden aber eine effektive Wahrnehmung des Auskunftsrechts. Darüber hinaus gibt es keinen Richtervorbehalt und keine nachträgliche Benachrichtigung.

Eine unzureichende Transparenz und ein ineffektiver individueller Rechtsschutz können verfassungsrechtlich nur durch eine besonders enge aufsichtliche Kontrolle ausgeglichen werden. Das setzt wirksame Befugnisse der Aufsichtsbehörden, eine lückenlose Protokollierung der Zugriffe und regelmäßigen Berichtspflichten an die Legislative voraus. Dennoch dürfte es für die Datenschutzbehörden schwer sein, eine derartige Datei effektiv zu kontrollieren. Bleibt abzuwarten, ob es gelingt.

Antiterrordatei einfügen
Rechtsrahmen national: Antiterrordateigesetz (ATDG)
Rechtsrahmen EU: Berichtspflichten nach Ratsbeschluss 2005/671/JI
Zweck: Terrorismusbekämpfung durch Ermöglichung von Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten mittels einer Verbunddatei
Erfasste Personen: ca. 13.000

Zweck
Inhalt
Zugriff
Verwaltung
Kontrolle
3
5
5
3
4
Gesamturteil: mangelhaft

MICHAEL KUHN *Jahrgang 1981, studierte Rechtswissenschaften an den Universitäten in Passau, Cardiff und der Humboldt-Universität in Berlin. Zu seinen Schwerpunkten gehören Europarecht, Staats- und Verwaltungsrecht sowie Datenschutz- und Internetrecht. Er promoviert gegenwärtig zum Recht auf Anonymität im Internet. 2013/2014 arbeitete er für die Humanistische Union am Projekt „Staatliche Datensammlung – Sind Bürger gefährdet?“.*

Anmerkungen:

https://www.humanistische-union.de/thema/datenschutz-index-fuer-sicherheitsdatenbanken/
Abgerufen am: 15.08.2024