Thilo Weichert

Die (un)heimlichen Datensammlungen
Von der Deutungsmacht und Deutungshoheit der Polizei

I. Einleitung

Es war für mich überraschend, dass ich im Jahre 2011 auf einem Strafverteidigertag zum Thema »un-heimliche polizeiliche Datenbanken« eingeladen wurde. Es ist mehr als 30 Jahre her, als die polizeiliche Datenverarbeitung für die kritische Öffentlichkeit noch heimlich und unheimlich war. Seitdem hat sich in fast jeder Hinsicht ein Wandel ergeben: Staatliches informationelles Vorgehen, einschließlich dem der Polizei, hat sich weitgehend aus dem hoheitlichen Arkanbereich verabschiedet. Die Sicherheitsbehörden generell und v.a. die Polizeien haben gesetzliche Grundlagen für ihr informationelles Handeln erhalten. Transparenz im polizeilichen Handeln gehört inzwischen zum Selbstverständnis der Polizei wie zur demokratischen Erwartung der Gesellschaft an diese. Zudem haben wir inzwischen ein Internet, für das es fast keine Geheimnisse mehr gibt. Heimlichkeit und erst Unheimlichkeit sollten also kein Problem mehr sein.

Die Themenstellung ist aber tatsächlich Ausdruck eines Defizites und eines Bedürfnisses: Als die Informationstechnik bei der Polizei Einzug hielt, war dies ein gesellschaftliches und politisches Ereignis. Dazu gemacht hat es in den 70er Jahren auch ein Präsident des Bundeskriminalamtes, der polizeilichen Einsatz von Informationstechnik zu einer Ideologiefrage überhöhte und hierbei auf kritische Resonanz bei einem linksliberalen technikkritischen Bürgertum stieß. Darstellungen und Erörterungen zu diesem Thema wurden zur Massenware. Dies hat sich heute geändert. Ein Grund hierfür liegt darin, dass sich die Diskussionen über polizeilichen IT-Einsatz von der wenig spektakulären Speicherung und Auswertung auf die sich revolutionär entwickelnde Datenerhebung verlagert hat. Der Einsatz von Lauschangriff, Online-Durchsuchung, DNA-Analyse, biometrische Mustererkennung, Funkortung u. v. m. ist spektakulärer und vor allem anschaulicher als die nicht minder revolutionäre Weiterentwicklung bei der informationstechnischen Speicher- und Auswertungstechnik. Zugleich haben sich die Menschen den Einsatz intelligentester Informationstechnik (IT) längst selbst angeeignet, weshalb es selbstverständlich erscheint, dass auch die Polizei diese nutzt. Relevant ist weiterhin, dass die öffentliche Aufmerksamkeit für IT sich insgesamt vom staatlichen auf den privaten Bereich verschoben hat.
Dies ändert nichts an dem Umstand, dass polizeilicher IT-Einsatz und vor allem der Einsatz von Datenbanken starke Auswirkungen auf die Menschen haben kön-

nen, die – aus welchen Gründen auch immer – in Kontakt zur Polizei kommen und deren Daten gespeichert werden oder bereits aus anderen Grund gespeichert sind. Dies gilt in besonderem Maße für von strafrechtlichen Ermittlungen betroffene Personen. Die automatisierte Informationsverarbeitung der Polizei schreitet rasant voran und hat Auswirkungen nicht nur auf das Recht auf informationelle Selbstbestimmung der Betroffenen, sondern auch auf deren Freiheitsrechte generell, die zunehmend eine digitale Dimension bekommen, sowie auf die Rechte im Strafverfahren. Diese Bedeutung wird bei den Strafverteidigern bisher selten hinreichend erfasst. Für diese ist zwar der Einsatz von IT für eigene Zwecke inzwischen selbstverständlich geworden ist; deren Ausbildung und Interesse fokussiert sich aber regelmäßig nicht auf das eher exotische Spezialgebiet des polizeilichen IT-Einsatzes. So sind Informationen über polizeiliche Datensammlungen zwar verfügbar, aber nicht in verfügbarer Form aufbereitet. Dieser Umstand führte dann wohl zu dem Thema beim Strafverteidigertag verbunden mit einer Bitte an mich, einen strukturierten Überblick sowie eine datenschutzrechtliche Bewertung zu geben

II.
Entwicklung der polizeilichen Datenverarbeitung

Auch wenn polizeiliche Datenverarbeitung technikgetrieben ist und die IT in jüngster Zeit Fortschritte gemacht hat, die vor wenigen Jahren noch nicht vorstellbare waren, lohnt es sich, einen kurzen Blick auf die Geschichte dieser Entwicklung zu werfen. Seit Bestehen der Kriminalpolizei gibt es Diebeslisten und Register auf Papier und Karteikarten. Mit der Bürokratisierung der Polizei haben sich die immer noch in Verwendung befindlichen Kriminalakten sowie als Findmittel Aktennachweise entwickelt. Da wir es bei vielen polizeilichen Informationsprozessen mit großen Datenmengen zu tun haben, fand die Automation hier früh Einzug. Schon in den 50er Jahren wurden automatisierte Lochkartenauswertungen bei der Polizei eingesetzt.

Die Informationsautomation der Polizei entwickelte sich in den 60er Jahren rasant und wird seitdem aus gutem Grund mit einem Namen in Verbindung gebracht: Horst Herold, der Präsident des Bundeskriminalamtes (BKA) von 1971 bis 1981, fand zum Amtsantritt eine unscheinbare Bundesbehörde vor und baute diese innerhalb von 10 Jahren zu einer schlagkräftigen Zentralstelle aus. Als Hauptinstrument für deren Arbeit und damit auch für deren Macht sollte eine zentralisierte informationstechnische Struktur sein, die sukzessive auf- und ausgebaut wurde. Zum Treibsatz dieser Entwicklung wurde die Bekämpfung des RAF-Terrorismus, der für die Zentralisierung und den sprunghaften Ausbau der Datenverarbeitung eine hervorragende Legitimation lieferte. Am 13.11.1972 wurde die INPOL-Fahndungsdatei

in Betrieb genommen und damit der Grundstein gelegt für eine Verbundstruktur zwischen Bund und Ländern mit dem BKA im Zentrum. INPOL steht seitdem als Kürzel für »das« bundesweite »Informationssystem der Polizei«. 1975 wurde eine Gesamtkonzeption INPOL vorgelegt, die in Teilen ihrer Grundstruktur bis heute Gültigkeit behalten hat.

Anfang der 80er Jahre, noch unter dem Einfluss von Herold, wurde eine zweite Generation der Datenverarbeitung geboren: Neben die hierarchischen Datenbanken traten komplexe relationale Verarbeitungsstrukturen, bei denen im Prinzip jede Information mit jeder anderen Information verknüpft werden können sollte. Auf Bundesebene wurden hierzu PIOS-Dateien (Personen, Institutionen, Objekte, Sachen) aufgebaut. Für komplexe Einzelfallermittlungen sowie bei umfassenderen Ermittlungszusammenhängen kamen SPUDOKs (Spurendokumentationen) zum Einsatz, in denen sämtlichen Erkenntnisse für alle beteiligten Ermittler verfügbar gemacht werden sollten. 1990 wurden Grundsätze der Zusammenarbeit zwischen Bund und Ländern bei INPOL verbindlich festgelegt.

INPOL war von Anfang erkenntnisbasiert, wobei zunächst vorrangig mit formatierten oder frei formulierten Texten gearbeitet wurde. Schon in den 80er Jahren eröffneten sich mit der Digitalisierung anderer Datenformate neue Möglichkeiten der Erfassung und Auswertung, für die die bisherige INPOL-Konzeption nicht angelegt war. Daher begannen 1988 Vorbereitungen für ein INPOL-neu, bei dem u. a. die Integration von flexiblen Datenformaten, also auch von Bildern, Ton, Mustern und Programmen angestrebt wurde. Mittels neuer Techniken und Verfahren sollten Verknüpfungen verschiedener Daten zweck- und funktionsübergreifende Auswertungen ermöglichen, die sowohl den Ermittler wie auch - in aggregierter Form - der Polizeiführung zur Verfügung gestellt werden sollten. Zunächst scheiterten wegen offensichtlich zu ehrgeizigen Funktionsanforderungen Versuche der Implementierung des neuen Systems. Im Jahr 2003 startete dann INPOL-neu mit einer weitgehend neuen Konzeption. Im Jahr 2006 wurde von INPOL-neu die Version 5.0 betrieben.

Diese Entwicklung bis zur heutigen Realität der polizeilichen Informationsverarbeitung ist nicht ohne Horst Herold vorstellbar. Dieser brachte nicht nur Zentralisierung und Automation auf den Weg, sondern entwickelte auch die Visionen hierfür, die bis heute ebenso fortwirken wie die hieran geübten Kritiken. Herolds Vision bestand darin, genügend kriminalitätsrelevante und gesellschaftliche Daten zu sammeln, um es der Polizei - im übertragenen Sinn - zu ermöglichen, vor dem Täter am Tatort zu erscheinen und ihn so an seiner Tat zu hindern. Ein Instrument hierzu war die Kriminalgeografie, mit der Kriminalität raumbezogen erfasst und prognostiziert werden sollte. Von der Sozialforschung sollten milieubezogene Daten geliefert werden, mit denen personen- und gruppenspezifische kriminalitätsfördernde bzw. -hindernde Merkmale erkundet werden sollten.

Diese Erkenntnisse sollten dann sowohl in vor- und fürsorgende Strukturentscheidungen wie in die individuelle Behandlung von Risikopersonen einfließen. Über prädiktive Kriminologie sollten täterbezogene Präventionsmaßnahmen ergriffen werden - ein Konzept, das man bis heute in Großbritannien in einem großen Umfang verfolgt.

Herold war sich dessen bewusst, dass sein Konzept nicht ohne umfassende Erfassung der Persönlichkeit vieler oder idealerweise von allen Menschen möglich wäre. Daher legte er einen großen Wert auf die Informatisierung der Kriminalitätsbekämpfung. Durch Zentralisierung der Informationen und deren wissenschaftlicher Auswertung sollten dann die Handlungsleitlinien für die Polizei erstellt werden, die zwar nicht zu einer Ausrottung, wohl aber zu einer Reduzierung der Kriminalität bis zu einem minimalen Bodensatz führen sollte. Diese ehrgeizige Zielsetzung war Hintergrund für den Ausbau des BKA und für die Etablierung von INPOL als Verbund mit einer Vielzahl von allgemeinen und speziellen Dateien. Der informationelle Ausbau erfasste auch die Fahndungs- und Ermittlungsformen, z. B. die elektronische Ausschreibung, die von Herold »erfundene« Rasterfahndung, die Schleierfahndung oder das Profiling. In einem Interview mit dem bekannten Strafverteidiger Sebastian Cobler, das im Jahr 1980 in der Zeitschrift Transatlantik veröffentlicht wurde, kennzeichnete Herold seine umfassende gesellschaftliche Vision als die eines »Sonnenstaates«.

Diese Vorstellungen und politischen Planungen provozierten bei vielen Menschen Abwehr und Kritik. Konservative Reaktionen richteten sich gegen die Zentralisierung. Im Vordergrund stand aber die Kritik des humanistisch und rechtsstaatlich argumentierenden linksliberalen Bürgertums, wonach das von Herold verfolgte paternalistische Gesellschaftsmodell zu Missachtung der kollektiven und individuellen Selbstbestimmung der Menschen führen würde. Den Kritikern gemeinsam war eine technikabwehrende Grundeinstellung. Diese Sichtweise war letztlich auch prägend für den Widerstand gegen die Volkszählungen 1983 und ´87, der zur Entscheidung des Bundesverfassungsgerichtes führte, in dem dieses aus dem allgemeinen Persönlichkeitsrecht rechtsfortbildend ein Grundrecht auf informationelle Selbstbestimmung ableitete.

Dieses neue Grundrecht war für die weitere Debatte um den IT-Einsatz bei Sicherheitsbehörden bestimmend. Es bedurfte nunmehr bei informationellen Eingriffen normenklarer kalkulierbarer Sicherheitsgesetze mit einklagbaren Betroffenenrechten. An Stelle der staatlichen Informationseinheit traten der Grundsatz der Zweckbindung und die informationelle Gewaltenteilung. Diese neue grundrechtliche Begrenzung hatte u. a. das Bestreben der Sicherheitsbehörden zur Folge, ihre bisherige Praxis der Informationsverarbeitung weitgehend gesetzlich abzusichern. Diese Ansätze einer Sicherheitsgesetzgebung provozierten wiederum einen umfangreichen gesellschaftlichen Diskurs über Sicherheitsinfrastruktur, über die justizielle Kontrolle der Polizei, über deren Transparenz. Ein Bestandteil dieses Diskurses war eine rechtswissenschaftliche Bearbeitung des Themas, der in Umfang und Tiefe bis heute einzigartig geblieben ist.

III. INPOL

Die Veröffentlichungen zu INPOL waren in den 80er und Anfang der 90er Jahre vielfältiger als die heutigen zu INPOL-neu. Dies bedeutet jedoch nicht, dass grundlegende Strukturinformationen heute gezielt seitens der Polizei geheim gehalten würden. Die Verbundteilnehmer sind bis heute im Wesentlichen die gleichen geblieben: BKA, Landeskriminalämter (LKÄ), Landespolizeien, Bundespolizei (ehemals Bundesgrenzschutz), Zoll mit Grenzkontrollaufgaben und Zollkriminalamt. Die folgende Aufzählung soll eine Augenblickaufnahme der aktuellen INPOL-Datenbestände liefern, wobei jedoch keine Festschreibung möglich ist, da sowohl die Inhalte, die Strukturen wie auch die informationellen Abläufe der miteinander verknüpften Systeme einem dauernden Änderungsprozess ausgesetzt sind. In den Klammern werden Umfangsangaben gemacht, die zumeist die Zahlen der erfassten Personen bzw. in Einzelfällen der vorhandenen Datensätze darstellen. Die Namen der Dateien sind oft selbsterklärend. Die Aufzählung ist nicht abschließend bzw. vollständig:

- Personenfahndung (4,4 Mio.)
- Kriminalaktennachweis (KAN, 4.3 Mio.)
- Innere Sicherheit (früher APIS, 1,5 Mio.)
- Haftdatei (500 T.)
- Violent Crime Linkage Analysis System (ViCLAS)
- DNS-Auskunftsdatei (DAD – Gendatenbank, 800 T.)
- Erkennungsdienst (ED, 5,9 Mio.)
- Automatisiertes Fingerabdruckidentifikationssystem (AFIS-P, 2,5 Mio.)
- APOK (Organisierte Kriminalität, 270 T.)
- Falldatei Rauschgift (FDR)
- Fedok (Finanzermittlungen, 7 T.)
- FUSION (Rockerkriminalität, 58 T.)
- Schleusungs-, Dokumentenkriminalität (DOMESCH, 120 T.)
- Gewalttäterdateien (u.a. LiMo 1,9 T., ReMo, AuMo)
- Gewalttäter Sport (11 T.)
- USA (11.09.2001, 80 T.)
- Kinderporno (47 T.)

Personengebundene Hinweise (PHW) sind besonders polizeirelevante Merkmale, die standardisiert und dateiübergreifend von der Polizei auf Bundes- und auf Landesebene genutzt werden. Diese dienen als Warn- und Handlungshinweise für die Polizisten beim Tagesgeschäft. Da sie aber sehr holzschnittartig Personen kennzeichnen, sind sie zugleich in höchstem Maße diskriminierungsträchtig, insbesondere im Hinblick auf ihre polizeiliche Nutzung, die oft mit staatlichen Zwangsmaßnahmen einhergeht. Da personengebunde Hinweise der stark verkürzte Ausdruck eines Sachverhalts, einer Situation oder einer Person sind, kommt es sehr darauf

an, dass diese Daten zutreffend sind. Der vor Ort im Einsatz befindliche Polizeibeamte muss sich bei spontan zu treffenden Eingriffsmaßnahmen auf die Richtigkeit der Daten verlassen können. Daher hat in den 80er Jahren die Konferenz der Innenminister der Länder (IMK) auf Drängen der Datenschutzbeauftragten Regelungen zur Erfassung und Speicherung von solchen personenbezogenen Hinweisen für die Polizeien verbindlich erlassen. Diese Regelungen geben vor, unter welchen Voraussetzungen und mit welchen Fristen personengebundene Hinweise in INPOL gespeichert werden dürfen. Im Übrigen hat sich die IMK im Einzelfall die Genehmigung neuer personengebundener Hinweise vorbehalten, was die Wichtigkeit der Regelungen unterstreicht.

Im Folgenden werden die in INPOL beim Bundeskriminalamt (BKA) verwendeten PHW dokumentiert:

§ 7 Abs. 3 BKAG: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; ANST, Ansteckungsgefahr; GEKR, Geisteskrank; BTMK, BtM-Konsument; FREI, Freitodgefahr; PROS, Prostitution; § 8 Abs. 2 BKAG: VEMO, Straftäter verbotener militanter Organisation/Vereinigung/Partei/ Gruppe; REMO, Straftäter rechtsmotiviert; LIMO, Straftäter linksmotiviert; AUMO, Straftäter politisch motivierter Ausländerkriminalität; EXPL, Explosivstoffgefahr; SEXT, Sexualtäter; HWAO, Häufig wechselnder Aufenthaltsort; § 7 oder § 8 BKAG, je nach Fallkonstellation: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; FREI, Freitodgefahr

IV.
Das BKA als Zentralstelle über INPOL hinaus

Neben den gemeinsamen Verbunddateien betreibt das BKA in eigener Regie und ausschließlich eigener Verantwortung Zentraldateien und Amtsdateien. Während die Zentraldateien eher bestimmte Deliktsgruppen oder zumindest Anlässe übergreifende Zwecke verfolgen, zielen Amtsdateien auf die Bereitstellung von Daten zu spezifischen Deliktsgruppen oder bestimmten Ermittlungszusammenhängen. Einige wenige Beispiele für die die sehr unterschiedlichen vielen Zentraldateien sind: BKA-Aktennachweis (2,2 Mio.), Globalisierung (IgaSt, 3 T.), ABC-Waffen (4 T.), VISA-Konsultation zentrale Behörden (2 Mio.), Islamischer Terrorismus (DABIS, 9 T. Pers., 3 T. Orga.). Beispiele für die ca. 100 BKA-Amtsdateien sind Sammlungen zu den Ermittlungsbereichen Nineeleven, Rauschgift, Geldwäsche, Untreue, Menschenhandel, Kindesmissbrauch, Personenschutz.

Die elektronische Datenverarbeitung der Polizei ist nicht abgeschottet von anderen Stellen. Es bestehen Schnittstellen, wobei regelmäßig die Polizei an fremden Datenbeständen teilhaben kann und Zugriffe auf externe Systeme nehmen kann. Der umgekehrte Fall, dass Externe auf Polizeidatenbestände zugreifen können, ist dagegen die Ausnahme, die dies z. B. bei begrenzten Zugriffen von Geheimdiensten der Fall ist.

Der Zugriff auf fremde Datenbestände soll der Polizei eine erweiterte Ermittlungsbasis sowohl bei der Strafverfolgung wie bei der Gefahrenabwehr eröffnen.

Das Ausländerzentralregister (AZR) dient vorrangig dem Informationsaustausch zwischen den unterschiedlichen im Ausländerrecht, also insbesondere im Aufenthalts- und im Asylverfahren zuständigen Stellen. Der Polizei kommen begrenzte eigene ausländerrechtliche Zuständigkeiten zu. Zugleich ist der umfassende Zugriff auch historisch begründet: Ausländerrecht wurde lange Zeit als besonderes Polizeirecht verstanden und hat sich erst in jüngster Zeit zum Aufenthaltsrecht emanzipiert.

Das Verständnis der Ausländerbehörden als besondere Polizeibehörden wie deren frühere begrenzte technische Kompetenz im Bereich der Biometrie führten dazu, dass das Automatisierte Fingerabdrucksystem auch insoweit beim BKA geführt wird, als es ausschließlich ausländerrechtliche Zwecke verfolgt (AFIS-A). Dies geht mit einer Zugriffsmöglichkeit der Polizei einher.

Das Bundeszentralregister (BZR) beim Bundesamt für Justiz (BAJ) dient der Auskunftserteilung über strafrechtliche Verurteilungen. Das Zentrale Verkehrsinformationssystem (ZEVIS) beim Kraftfahrtbundesamt (KBA) gibt umfassend Auskunft über zugelassene Kraftfahrzeuge und über Fahrerlaubnisse sowie über Verkehrsverstöße, was für die Polizei als Verkehrsordnungsbehörde von hoher Relevanz ist.

Der Zugriff der Polizei auf die Kontodatenbestände bei sämtlichen deutschen Finanzinstituten, die über das Bundeszentralamt für Steuern vermittelt wird, ist materiell-rechtlich beschränkt auf die Aufklärung bestimmter schwererer Straftaten.

Mit der Europäisierung vieler Ordnungsaufgaben, der bisherigen dritten Säule der EU, wurden auf der Ebene der Europäischen Union (EU), die mit dem Vertrag von Lissabon organisatorisch, politisch und rechtlich vollständig in die EU integriert wurde, bestehen inzwischen parallel zu den nationalen europäische Datenbestände, zu denen die Polizei Zugriff hat. So besteht entsprechend zu AFIS-A in Straßburg die Datei EURODAC (266 T.). Das Schengener Informationssystem SIS versteht sich u. a. als Sicherheitskompensation für und damit als die Antwort auf die Abschaffung der Grenzkontrolle und ist im Ergebnis mit einer europäischen Fahndungsdatei (z. B. Personenfahndung 110 T.) vergleichbar.

Beim Europäischen Polizeiamt (Europol) in Den Haag werden neben dem Europol-Informationssystem Arbeitsdateien zu Analysedateien sowie das Europäische Informationssystem (EIS) geführt. Schließlich ist das BKA nationale Zentralstelle für die weltweite Polizeizusammenarbeit über die in Paris sitzende Organisation Interpol. Interpol betreibt Recherche und Fahndungsdateien, die vom BKA aus online gespeist und von denen Abrufe getätigt werden können.

V. Sonstige Polizeidatenverarbeitung

In den Bundesländern bestehen ähnlich zu den Zentral- und Amtsdateien beim BKA in den Landeskriminalämtern (LKÄ) viele Spezialdateien mit landesweiter Bedeutung, z. B. Register über Sexualstraftäter oder vielfältige Analyse- und Auswertedateien. Für die Kommunikation mit den anderen Ländern und den Bundespolizeibehörden wird die INPOL-Verbundstruktur verwendet.

Inzwischen hat die elektronische Datenverarbeitung die Schreibmaschine bis hinein in die einzelnen Polizeireviere verdrängt. In den meisten Bundesländern bestehen elektronische Vorgangsbearbeitungs- und -dokumentationssysteme (z.B. IGVP Bay, @rtus SH), die das polizeiliche Handeln dokumentieren, für Auskunftszwecke genutzt werden und die zunehmend für die Auswertung und Analyse zu unterschiedlichen Zwecken genutzt werden können. Zumindest erwähnt werden müssen weiterhin Leitstellen, bei denen die Polizei oft in Kooperation mit den zumeist kommunal organisierten Rettungsdiensten Notrufzentralen betreiben.

Die informationstechnische Kooperation der Polizei mit den Geheimdiensten, die sich lange Zeit auf geringe Datenzugriffsmöglichkeiten beschränkten, hat nach dem 11. September 2001 neuen Auftrieb erhalten. Es wurde ein Antiterrordateigesetz verabschiedet, auf dessen Basis eine gemeinsame Antiterrordatei und Projektdateien geführt werden. Die gesetzliche Grundlage dieser Kooperation wird derzeit vom BVerfG verfassungsrechtlich überprüft.
Eine informationelle Zusammenarbeit zwischen Polizeien und Geheimdiensten erfolgt außerdem über die Gemeinsamen Lagezentren GIZ, GTAZ, GASIM.

VI. Entwicklungen

Die Informatisierung der Polizei kann durch vier Trends beschrieben werden: 1. die Europäisierung bzw. Internationalisierung, 2. die Vergeheimdienstlichung, 3. die technische Weiterentwicklung und 4. die Einbeziehung Privater.

Für den ersten Trend steht der Aufbau der Schengenstruktur mit dem SIS, von Europol und Eurodac, der direkte multinationale polizeiliche Datenaustausch über den Vertrag von Prüm sowie die Umsetzung des Stockholmer Programms. Auch Bestrebungen zur europaweiten Datensammlung für Sicherheitszwecke aus den Bereichen Telekommunikation, Flugverkehr und Bankentransaktion steht hierfür. (Euro-PNR, Euro-TFTP). Diese letztgenannten Datensammlungen haben ironischerweise einen transatlantischen Ursprung, nämlich die Kooperation mit Sicherheitsbehörden in den USA, die nun europäische Begehrlichkeiten begründeten (PNR, SWIFT/TFTP)

Die Vergeheimdienstlichung der Polizei hat eine lange Tradition. Immer hat die Polizei in bestimmten Bereichen verdeckte bzw. heimliche Ermittlungen durchgeführt. Diese Tradition wurde zwar teilweise durch die Separierung der Geheimdienste von der Polizei und durch eine verstärkte demokratische Kontrolle und rechtsstaatliche Kontrollierbarkeit der Polizeitätigkeit in Frage gestellt (Trennungsgebot). Mit der Bekämpfung des internationalen Terrorismus haben Polizei und Nachrichtendienste heute aber wieder ein wirksames Legitimationsmuster für geheimes Vorgehen und für eine intensivere Form der informationellen Zusammenarbeit gefunden.

Weiterentwicklungen der Technik werden von Sicherheitsbehörden allgemein wie von der Polizei konkret für die eigenen Ermittlungen genutzt. Mit der genetischen Identifizierungsmöglichkeit wurden entsprechende Dateien, z. B. die DNA-Datei beim BKA aufgebaut. Von den Dateien AFIS und DAD ausgehend finden biometrische Zuordnungen durch die Polizei in jeder denkbaren Form statt. Die vielfältigen neuen Spuren im Internet werden durch die Polizei für ihre Aufgabenwahrnehmung genutzt. Die Auswertung zur Verfügung stehender Daten in sog. Data-Warehouses eröffnet erheblich erweiterte Erkenntnismöglichkeiten, da als Datenbasis Informationen herangezogen werden können, die zunächst für einen anderen Zweck erhoben und gespeichert wurden.

Auch die Einbeziehung Privater in polizeiliche Ermittlungen hat schon eine längere Tradition. Neu ist, dass die Privaten gesetzlich verpflichtet werden, ausschließlich für Ermittlungszwecke bei sich anlässlich ihrer Geschäftstätigkeit anfallende oder erhebbare Daten aufzubewahren, so wie es bei der Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten der Fall ist, bei der Weitergabe von sog. Passenger Name Records (PNR - Fluggastdaten) oder von internationalen Banktransaktionsdaten des belgischen Dienstleisters SWIFT über Europol an US-Behörden.

VII. Rechtsgrundlagen

Nach dem Volkszählungsurteil 1983 mussten die polizeilichen Informationseingriffe auf bereichsspezifische normenklare gesetzliche Grundlagen gestellt werden. Mit dem Aufkommen neuer technischer Ermittlungsmöglichkeiten hatte das eine umfassende gesetzliche Neuregulierung zu Folge. Die Grundlagen finden sich regelmäßig im spezifischen Sicherheitsrecht, also z. B. im Bundeskriminalamtsgesetz (BKAG), im Bundespolizeigesetz, im Zollfahndungsdienstgesetz oder in der Strafprozessordnung (§§ 474 ff. StPO). Daneben fanden einige Regelungen Eingang ins allgemeine Datenschutzrecht.

Die Rechtsgrundlagen für die Datenverarbeitung der Landespolizeien zum Zweck der Gefahrenabwehr finden sich in den Landespolizeigesetzen (Schleswig-Holstein:

Landesverwaltungsgesetz, mehrere andere Länder Sicherheits- und Ordnungsgesetz). Werden mit einer Datenverarbeitung sowohl strafverfolgende wie auf gefahrenabwehrende Zwecke verfolgt, so geht gemäß § 483 Abs. 3 StPO das Polizeirecht vor.
Da die gesetzlicher Verarbeitungsgrundlagen wegen der rasanten technischen Entwicklung und den sich ändernden Anforderungen nur allgemeinen Charakter haben können, besteht bei Polizeidateien das gesetzliche Erfordernis der Konkretisierung durch Errichtungsanordnungen und/oder durch Rechtsverordnung. Bei Errichtungsanordnungen handelt es sich um Verwaltungsvorschriften, in denen die in Dateien verarbeiteten Datenkategorien, der Datenumfang, deren Zweck, deren Organisation und die Nutzung konkretisiert werden. Diese Errichtungsanordnungen sind in der Regel nicht öffentlich, sondern häufig als VS-nfD (Verschlusssache - nur für den Dienstgebrauch), teils sogar höher eingestuft, was insbesondere für die Dateianordnungen der Nachrichtendienste zutrifft.

§ 7 Abs. 6 BKAG verpflichtet beim Betrieb von Verbunddateien zum Erlass einer Rechtsverordnung, welche die Einbindung in den Verbund und die Art der Daten festlegt. Solche Rechtsverordnungen wurden über viele Jahre hinweg nicht erlassen. Anlässlich der Prüfung der Rechtmäßigkeit der Verarbeitung in der Verbunddatei Gewalttäter Sport stellte am 22.05.2008 das Verwaltungsgericht (VG) Hannover und mit Urteil vom 16.12.2008 das Oberverwaltungsgericht (OVG) Niedersachsen klar, dass es sich bei dem Erfordernis einer wirksamen Rechtsverordnung nicht um eine reine Ordnungsvorschrift handelt, sondern dass diese Bedingung für eine rechtmäßige Verarbeitung ist. Das Revisionsverfahren gegen diese Urteile wurde so lange herausgezögert, bis am 04.06.2010 eine allgemeine Rechtsverordnung erlassen worden ist, die am 09.06.2010 in Kraft trat. Noch am gleichen Tag, also am 09.06.2010, urteilte das Bundesverwaltungsgericht (BVerwG) dann, dass die Datenspeicherung jetzt rechtmäßig sei.

Generell und besonders bei der polizeilichen Datenverarbeitung gilt das Zweckbindungsprinzip, also dass Daten grundsätzlich nur für den bei der Erhebung verfolgten Zweck weiterverarbeitet werden dürfen. Dieser Grundsatz wird weitgehend durch § 481 StPO aufgehoben. Danach wird für sämtliche Zwecke der Gefahrenabwehr und der Strafverfolgung eine Art »Zweckglocke« normiert, also ein einheitlicher Zweck fingiert. Etwas anderes gilt nur, wenn besondere Regelungen bestehen, was z. B. bei besonderen, v. a. heimlichen Ermittlungsmethoden sehr oft der Fall ist.

Die Zweckglocke ändert aber nichts an dem Umstand, dass bei den konkreten Maßnahmen der polizeilichen Datenverarbeitung hinsichtlich der Zwecke jeweils präzise differenziert werden muss. Insbesondere nach dem Bundes- bzw. Landespolizeirecht ist sauber zu unterscheiden zwischen der Gefahrenvorsorge, der Gefahrenabwehr, der Vorsorge zur Verfolgung künftiger Straftaten sowie der Vorgangsbearbeitung und Vorgangsdokumentation. Auch die beiden letztgenannten

Verarbeitungsformen erfolgen inzwischen weitgehend elektronisch mit dem Trend, weitgehend auf Papier verzichten zu können.

Wegen der erwähnten »Zweckglocke« und den äußerst differenzierten speziellen Zweckbindungen spielt die Erforderlichkeitskontrolle beim Datenzugriff eine zentrale Rolle (Grundsatz des »need to know«). Hierbei handelt es sich um durch die Aufgabenstellung der jeweiligen Polizisten begrenzten Zweckbindungen, die technisch durch Zugriffsbeschränkungen sichergestellt sein sollten. Die Erforderlichkeitskontrolle hat neben der funktionalen auch eine räumliche Dimension, was die Zugriffsbeschränkung innerhalb der Dienststelle, innerhalb der Region bei örtlichen Vorgängen sowie innerhalb eines polizeilichen Organisationsbereiches (z.B. Direktion) nötig machen kann.

Werden darüber hinausgehend automatisierte Auswertungen für Zwecke der Führung, der Organisation und Planung oder allgemein der Statistik vorgenommen, so müssen diese auf anonymisierter Basis erfolgen.

Wegen der äußerst komplizierten Zwecke- und Erforderlichkeitsstruktur bei zugleich umfassender Vernetzung kommt der materiellen Rechtmäßigkeit polizeilicher Datenverarbeitung generell besondere Bedeutung zu. Neben den manchmal nur schwer eindeutig zu beantwortenden materiellrechtlichen Fragen gibt es aber immer wieder strukturell rechtswidrig angelegte Formen der Datenverarbeitung. Beispiele hierfür ist die erwähnte Datenweitergabe von SWIFT-Daten an US-Sicherheitsbehörden über Europol, die eindeutig hinter verfassungsrechtlichen Anforderungen zurückbleibt. Weitere solche Beispiele für offensichtlich rechtswidrige Datenspeicherungen sind die 3.000 wegen Beleidigungen gespeicherten Datensätze in DAD, also der DNA-Datenbank. Schon vom Deliktstyp her, kann die Erwartung, dass der Beschuldigte „Straftaten von erheblichen Bedeutung" begehen wird und hierbei die DAD zur Aufklärung geeignet sein muss - unabhängig von der Frage der Angemessenheit - nicht die Speicherung rechtfertigen. Ein weiteres - eher exotisches - Beispiel ist die Speicherung von Geruchsproben von G8-Gipfel-Gegnern beim BKA.

Angesichts der vielen rechtlichen Fragestellungen und unklaren Grenzziehungen ist es erstaunlich, dass die rechtliche Anfechtung der polizeilichen Datenverarbeitung durch die Betroffenen oder die Thematisierung in Verfahren, evtl. unter dem Gesichtspunkt des Verwertungsverbotes, nur selten erfolgt.

VIII. Datenqualität

Für jede personenbezogene Datenverarbeitung gilt, dass Daten richtig und erforderlich sein müssen. Wegen der starken exekutiven Bedeutung von Polizeidaten gilt dies besonders. Dies hat zur Folge, dass vor jeder Datenerhebung und -verarbeitung von der verantwortlichen (Daten verarbeitenden) Stelle eine Relevanz- und Qualitätsprüfung durchgeführt werden muss.

Bei Daten über abgeschlossene Strafverfahren ist hinsichtlich der verfahrensrechtlichen (gerichtlichen) Gesichertheit der Daten zu unterscheiden zwischen Verurteilung, Freispruch 1. (erwiesene Unschuld) und 2. Klasse (mangels Beweis), Einstellung nach den §§ 153/153a StPO mit einer wenig verifizierten Schuldvermutung, und nach 170 Abs.2 StPO wegen fehlendem Anlass zur Erhebung öffentlicher Anklage.

Weiterhin kann unterschieden werden zwischen objektiven Tatsachenfeststellungen (sog. harten Daten) und sog. weichen Daten, die unsichere Schlussfolgerungen aus Tatsachen, Verdächte, Vermutungen und bloße Hypothesen sein können. Die Grenzen zwischen harten und weichen Daten sind oft fließend und hängen von der subjektiven Wahrnehmung des Sachbearbeiters ab. Werden unzutreffende Schlüsse gezogen, so besteht die Gefahr der Falschverdächtigung der Betroffenen. Eine weitere relevante Differenzierung erfolgt nach Sensibilität der Daten. Diese kann sich aus dem Inhalt ergeben, etwa wenn besondere Datenkategorien betroffen sind (Gesundheit, Sexualität, politische Überzeugung..., vgl. § 3 Abs. 9 BDSG), aus der Art der Quelle, etwa wenn ein Sozial- oder Berufsgeheimnis erfasst wird, oder aus der Art der Ermittlungsmaßnahme (z.B. Einsatz heimlicher technischer Mittel. Daten mit Kernbereichsbezug sind besonders heikel; reine Kernbereichsdaten dürfen nicht gespeichert werden.

Die Polizei erfüllt mit der Akteneinsicht und der Auskunftserteilung nicht nur eine Aufgabe gegenüber den Betroffenen. Diese Informationsrechte sind nicht nur grundrechtlich begründet; ihre Inanspruchnahme hat auch eine Auswirkung auf die Qualität der Daten, da dem Betroffenen nur so die Möglichkeit gegeben werden kann, die Richtigkeit und Rechtmäßigkeit zu überprüfen und evtl. zu reklamieren. Über die Berichtigung, Sperrung oder Gegendarstellung erfolgt eine Qualifizierung der Daten.

Ein weiterer für die Datenqualität relevanter Aspekt sind der Kontext der Erhebung und die Dokumentation der Quelle. Der Kontext sollte, die Datenquelle muss (z. B. als Metadatum, über Eingabeprotokolle) mitgespeichert werden, um im Nachhinein Relevanz und Qualität der Daten überprüfen zu können.

Weiteres rechtlich relevantes Differenzierungskriterium bei der Datenspeicherung ist der Betroffenenstatus. Im Folgenden sollen einige relevante Rollen aufgezählt werden, weshalb eine Speicherung erfolgte: Straftäter, Beschuldigter, Straftatverdächtiger, Gefährder/Störer, Zeuge, Hinweisgeber, Opfer, gefährdete Person, vermisste/unbekannte/hilflose Person, Toter, Kontakt- und Begleitperson, Hilfsperson und sonstige dritte Person. Je nach Rolle der Person können unterschiedliche Speicherungsfristen in Betracht kommen. Diese sind teils gesetzlich vorgegeben; in Fällen, in denen das Gesetz einen Ermessensspielraum bei der Beurteilung der Speicherungsdauer einräumt, muss eine prüffähige Interessenabwägung durch die verantwortliche Stelle vorgenommen und dokumentiert werden.

Die exemplarisch genannten Kriterien, die Datenqualität beschreiben, sind primär als Werkzeuge anzusehen, mit denen die Polizei im Eigeninteresse großzügig umgehen kann. Die Rechtmäßigkeit, die Aussagekraft und die Effektivität der Datenverarbeitung hängen in erheblichem Umfang von dem Ergebnis steter Qualitätssicherungsmaßnahmen ab.

IX.
Data-Warehouses

Die Polizei ist bestrebt, die bei ihr vorhandenen Daten möglichst umfassend zu nutzen. Zur Erreichung dieses Zieles bieten sich technisch Data-Warehouse-Lösungen an. Dabei werden sämtliche vorhandenen Daten – unabhängig von den jeweiligen Zwecken – in einer gemeinsamen Datenbank abgelegt. So können Verknüpfungen von Daten sowie anwendungsübergreifende Auswertungen einfach vorgenommen werden. Data-Warehouses ermöglichen technisch eine zweckübergreifende Datennutzung und zielen oft hierauf ab. Damit stehen sie tendenziell im Konflikt mit dem auch im Polizeibereich geltenden datenschutzrechtlichenZweckbindungsprinzip.

Von zentraler Bedeutung bei einer Warehouse-Datenverarbeitung ist die Qualität der eingegebenen Daten (s. o. Nr. VIII). Fehler können sich gravierend auswirken, auch weil sich diese bei jeder Nutzung, Verknüpfung oder Auswertung fortschreiben. Dies bedingt, dass weitere Maßnahmen zur Sicherstellung der Datenqualität nötig sind.

Weiterhin bedarf es beim Aufsetzen von (Polizei-) Data-Warehouses einer Vielzahl technisch-organisatorisch-rechtlicher Festlegungen, die aus Nutzungsszenarien abgeleitet werden sollten (z. B. technische Zugriffs- und Auswertungsvorgaben, Rollenfestlegungen, Dienstanweisungen). Damit sind die jeweiligen gesetzlichen Zweckbegrenzungen abzubilden. Bei diesen Festlegungen müssen funktionale Anforderungen an die Bedarfsträger gestellt werden; je nach Aufgabe sind Rollen zu definieren, aus denen dann die Berechtigungen abgeleitet werden, deren Beachtung technisch-organisatorisch sichergestellt werden muss. Dabei kann es sich als sinnvoll und geboten erweisen, nach Zwecken, Regionen oder anderen Begrenzungen Data-Marts, also Teildatenbestände zu separieren. In jedem Fall geht bei Warehouse-Lösungen kein Weg vorbei an der Zuspeicherung von Metadaten, die Zwecke, Funktionen, Lese- und Schreib- und Auswerteberechtigungen steuern. Fehlen solche wirksamen Begrenzungen, so ist der Betrieb des Warehouses unzulässig.

Besonders heikel sind in Warehouses Recherchemöglichkeiten in Freitexten und unstrukturierten Vorgangsdokumentationen, da nicht gewährleistet werden kann, dass jeweils sämtliche genutzten Daten zur Aufgabenerfüllung auch tatsächlich erforderlich und deren Nutzung damit zulässig ist. Für die Auswertung solcher Datenbestände müssen Vorgaben vordefiniert werden (z. B. über Black- und Whitelists).

Bei den präzise vorzunehmenden Rollen- und Aufgabenbeschreibungen in Polizei-Warehouses kann regelmäßig grob zwischen folgenden Funktionen unterschieden werden: Super-User mit umfassenden Kompetenzen, Experten in Zentralstellen der Polizei mit begrenzten Zugriffsrechten auf fremde Daten und Sachbearbeiter mit Zugriffsrechten nur auf die Daten der eigenen Dienststelle. Gemäß der höheren Gefährdung bei umfassenderen Rechten muss hier auch eine höhere Kontrolldichte gewährleistet sein.

Generell gilt bei polizeilichen personenbezogenen Warehouses, dass darin kein Data-Mining erfolgen darf, also eine Auswertung der Daten nach noch nicht vorher festgelegten Fragestellungen. Vielmehr müssen sich sämtliche Nutzungen am Erforderlichkeitsgrundsatz orientieren. Ist ein einzelnes Datum für vorgesehene polizeiliche Zwecke nicht mehr nötig, so muss es gelöscht werden, was voraussetzt, dass nicht nur ein ganzer Datensätze, sondern auch jedes Einzeldatum technisch gelöscht werden kann. Organisatorische Erforderlichkeitsregeln genügen nicht, vielmehr sind bei derart komplexen Anwendungen wie Warehouses neben den materiellrechtlichen auch Vorgaben zur technischen Ausgestaltung rechtlich geboten.

X.
Generelle Anforderungen an polizeiliche Datenspeicherungen

Nicht nur für Warehouses, aber dort besonders gilt, dass bei jeder Datennutzung (=Befassung mit dem Vorgang und somit auch mit dem Datensatz) durch den Sachbearbeiter eine Relevanzprüfung erfolgen muss, nicht nur aus funktionalen, sondern auch aus bürgerrechtlichen Gründen. Dies schließt mit ein, dass bei jeder Vorgangsbearbeitung im Einzelfall eine kurze implizite Prüfung erfolgt, ob das Datum bzw. der Datensatz überhaupt noch zur Aufgabenerfüllung geeignet und erforderlich ist. Ist dies nicht (mehr) der Fall, muss das Datum, unabhängig von sonstigen Prüf- oder Löschfristen, gelöscht werden.

Für Polizeidatenbestände gelten im Allgemeinen folgende Aussonderungsprüffristen: Erwachsene bis zu 10, Jugendliche bis zu 5, Kinder bis zu 2 Jahren. Nach Fristablauf muss, wenn ein Datensatz weitergeführt werden soll, eine dokumentierte Einzelprüfung erfolgen. Es darf keine automatischen Fristverlängerungen geben. In der Vergangenheit galt, dass nur jeder 10. Datenabruf in polizeilichen Auskunftssystemen protokolliert werden musste. Hintergrund dieser Regelung war, dass für die Protokollierung nicht genügend Speicherplatz zur Verfügung stand, die Auswertung von Logfiles äußerst aufwändig war und die Zweckbindung der Protokolldatenbestände nur schwer sichergestellt werden konnte. Diese technischen Beschränkungen bestehen heute nicht mehr. Das gleiche gilt für das in diesem Kontext oft angeführte Kostenargument hinsichtlich des notwendigen

Speicherplatzes. Dies bedeutet, dass praktisch jede Form der polizeilichen Datenverarbeitung mitgeloggt und nach bestimmten Plausibilitätskriterien regelmäßig technisch ausgewertet werden muss. Die Pflicht zur Vollprotokollierung gilt nicht nur für den Schreibenden, sondern auch für den lesendem Zugriff auf Daten (§ 11 Abs. 1 S. 1 BKAG). Dies wird teilweise in der Praxis noch bestritten. Die Protokolldatenbestände sind, auch für Zwecke der händischen Kontrolle im Einzelfall, in der Regel zumindest ein Jahr lang aufzubewahren.

Die Protokolldaten unterliegen einer strengen Zweckbindung und dürfen grundsätzlich nur für Zwecke der Datensicherheit, der Datenschutzkontrolle und zur Sicherstellung des Systembetriebs genutzt werden. Nur in eng definierten Ausnahmefällen ist eine Nutzung für Polizeizwecke erlaubt.

Erfolgt eine elektronische personenbezogene Datenspeicherung mit Aktenrückhalt, sind also erläuternde, vertiefende oder beweissichernde Informationen in einer Papierakte abgelegt, so muss bei der elektronischen Speicherung dieser Aktenbezug im elektronischen Datenbestand klar erkennbar sein. Umgekehrt muss sich aus der Papierakte ergeben, in welchen elektronischen Datenbeständen die hinterlegten Daten nachgewiesen werden. Bei einer rein elektronischen Vorgangsbearbeitung muss der gesamte Kontext des Vorgangs nachvollziehbar und aus sich selbst heraus verständlich dokumentiert sein.

Bei sämtlichen Formen polizeilicher Datenverarbeitung, insbesondere bei Warehouse-Anwendungen sind nach Neueinführung, aber auch im Betrieb regelmäßig (z.B. nach 3 Jahren) Verfahrensevaluierungen vorzunehmen.

XI.
Auskunftserteilung

Für die Betroffenen gibt es unterschiedliche rechtliche Wege, Auskunft über die zur eigenen Person gespeicherten Polizeiinformationen zu erhalten. In § 147 StPO ist die Akteneinsicht des Verteidigers geregelt, dessen Zielrichtung insbesondere in der Gewährleistung eines fairen Verfahrens für den Betroffenen bzw. Beschuldigten liegt. Vor Abschluss des Ermittlungsverfahrens kann die Einsicht verweigert werden, wenn mit ihr der Untersuchungszweck gefährdet würde.

Unabhängig daneben besteht ein höchstpersönlicher datenschutzrechtlicher Auskunftsanspruch des Betroffenen (vgl. § 19 BDSG). Eine pauschale Begründung einer Auskunftsverweigerung ist unzulässig; in jedem Fall muss eine sich aus dem Einzelfall ergebende Begründung vorliegen, bei der eine Interessenabwägung erfolgt.

Bei Verbunddateien, also in allen Fällen des INPOL-Verbundes, besteht eine Weiterleitungspflicht an die verantwortliche Stelle nach § 6 Abs. 2 BDSG. Von Seiten der Sicherheitsbehörden wird die bürgerfreundliche Umsetzung dieser Regelung

oft erschwert, was für die Betroffenen zu einer Rechtsverkürzung führen kann. Umso wichtiger sind die Kontrollmöglichkeit der jeweils zuständigen unabhängigen Datenschutzkontrollinstanzen, also des jeweiligen Landesbeauftragten für Datenschutz (LfD) bzw. des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Im Fall einer vollständigen oder teilweisen Auskunftsverweigerung kann sich ein Betroffener dorthin wenden und so zumindest eine externe Überprüfung der Zulässigkeit der Datenverarbeitung wie auch der Auskunftsverweigerung veranlassen.

XII.
Lokale Schnittstellen

Die personenbezogene Datenverarbeitung der Polizei wäre unvollständig beschrieben, wenn die regionale Vernetzung der Polizei mit anderen Stellen und Behörden unerwähnt bliebe. So hat die Landespolizei oder die örtliche Polizei in der Regel direkten lesenden Zugriff auf die Bestände der Melderegister oder auf Spiegeldatenbanken (Kopien) der Melderegister.

Zugriff wird weiterhin der örtlichen Polizei und Ordnungsbehörden in vielen Fällen auf das Personalausweis- und/oder Passregister gewährt. Hierbei geht es insbesondere um den Zugriff auf die dort abgelegten Gesichtsfotos, z. B. zur Identifizierung von Kfz-Fahrer bei Verkehrsverstößen.

Eine technische Kooperation erfolgt weiterhin, in den Bundesländern unterschiedlich, in bzw. mit Rettungsleitstellen, also mit der Feuerwehr, der medizinischen Notfallversorgung und dem Katastrophenschutz.

Keine technische Verknüpfung besteht zwischen Polizei und Staatsanwaltschaft. Die jeweils andere Stelle kann also nicht auf die elektronischen Datenbestände des jeweiligen Partners im strafrechtlichen Ermittlungsverfahren zugreifen. Zu nennen ist aber die Schnittstelle zu staatsanwaltschaftlichen Verfahren wie z. B MESTA; über diese werden Informationen wie das Aktenzeichen der Staatsanwalt und der Verfahrensausgang an die Polizei gegeben.

Eine systematische Nutzung der Polizeidatenbestände erfolgt aber für Sicherheitsüberprüfungen, im Rahmen von sonstigen Zuverlässigkeitsüberprüfungen, z. B. der Akkreditierung von Pressevertretern bei Großveranstaltungen, sowie bei bestimmten Einstellungsverfahren.

XIII.
Datenabgleich und Rasterfahndung

Besondere Formen der polizeilichen Datenauswertung sind der interne und der externe Datenabgleich. Letzteres wird mit dem Begriff der Rasterfahndung beschrieben. Die Rechtsgrundlagen hierfür finden sich in den §§ 98a ff. StPO sowie

im Polizeirecht des Bundes und der Länder (z. B. § 20j BKAG, §§ 195, 195a LVwG SH). Zielrichtung der Datenabgleiche ist es, eine Straftat bzw. eine Gefahrenlage aufzuklären oder den Aufenthalt einer Fahndungszielperson festzustellen. Der polizeiinterne Abgleich von Datenbeständen ist (z. B. nach § 98c StPO) unter geringen Voraussetzungen zulässig, wenn die dabei eingeführten Daten keinen besonderen gesetzlichen Verwendungsregelungen, also speziellen Zweckbindungen, unterworfen sind. Ungeschriebene Voraussetzung jeden Datenabgleichs ist die Beachtung der Grundsätze der Erforderlichkeit und besonders der Verhältnismäßigkeit.

Die externe Rasterfahndung nach den §§ 98a, 98b StPO bzw. nach den Polizeigesetzen ist voraussetzungsvoller. Bei ihr werden in besonderem Maße Daten von Unverdächtigen mit einbezogen, die in polizeilichen oder in fremden – privaten wie auch öffentlichen – Datenbanken registriert sind. Basis jeder Rasterfahndung ist eine Hypothese zur Verdachtsgewinnung bzgl. des Vorliegens bestimmter personenbezogener oder -beziehbarer Merkmale. Die Anordnungsbefugnis liegt bei einem Richter, nur bei Gefahr im Verzug bei der Staatsanwaltschaft bzw. der Behördenleitung im Bereich des Polizeirechts.

Für die Geeignetheit der Maßnahme müssen tatsächliche Anhaltspunkte für eine Gefahrenlage bzw. für eine Straftat von erheblicher Bedeutung bestehen. Besonders geschützte Daten dürfen nicht einbezogen werden. Spätestens nach Beendigung der Maßnahme ist die zuständige Datenschutzkontrollinstanz über die Maßnahme zu benachrichtigen.

Nach den terroristischen Anschlägen am 11.09.2001 wurde seit vielen Jahren wieder zum ersten Mal eine Rasterfahndung durchgeführt, um »terroristische Schläfer« ausfindig zu machen. Als Merkmale zur Verdachtsgewinnung wurden festgelegt: unauffälliges Verhalten, männlich, Alter zwischen 18 und 40, Student, Moslem, geboren in Staat mit islamischer Bevölkerung. Die Datenbeschaffung erfolgte bei Universitäten, Meldebehörden und dem Ausländerzentralregister (AZR). Abgleiche wurden vorgenommen mit Daten von Fluglizenzen, aus Atomgesetz-Zuverlässigkeitsüberprüfungen. Abklärungen sind teilweise auch bei Arbeitgebern vorgenommen worden.

Das in diesem Verfahren angerufene Bundesverfassungsgericht stellte im Jahr 2006 fest, dass zwar die rechtliche Grundlage für die Durchführung der Rasterfahndung verfassungskonform ist, die tatsächlichen Voraussetzungen für die verfassungskonform ausgelegten Tatbestände aber nicht vorlagen (BVerfG, B. v. 04.04.2006, 1 BvR 518/02). Dabei nahm das BVerfG eine Abwägung zwischen der Eingriffsschwere und den verfolgten Schutzzielen vor und stellte fest, dass es sich bei der Abwehr einer Gefahr für Bestand und Sicherheit von Bund und Ländern oder für Leib, Leben und Freiheit um hochrangige Verfassungsgüter handelt. Es wies auf die Gefahren für die Betroffenen hin, dass bei der Auswertung

der sensiblen Daten Diskriminierung droht bzw. Maßnahmen ergriffen werden können, die nachteilige Auswirkungen für die Betroffenen haben können bis hin zur Stigmatisierung. Neben dieser individuellen betonte das BVerfG auch die gesellschaftliche Relevanz der Maßnahme wegen deren Streubreite und wegen der Einschüchterungseffekte, die ganze Bevölkerungsgruppen treffen können. Zur Sicherstellung der Grundrechtskonformität betonte das BVerfG die Bedeutung von rechtlichen Vorkehrungen, insbesondere von Verfahrenssicherungen sowie die Gewährleistung individueller und gesellschaftlicher Transparenz.
Das BVerfG beanstandete nicht das der Maßnahme zu Grunde liegende Gesetz, sondern die Maßnahme selbst. Die rechtlich geforderte konkrete Gefahr setzt ein tatsachenbasierte Wahrscheinlichkeitsprognose voraus, die im vorliegenden Fall fälschlich positiv ausfiel.

XIV.
Prüfschema

Bei einer rechtlichen Überprüfung von polizeilichen Datenspeicherungen sind folgende Punkte relevant:

- Welche polizeiliche Aufgabe wird damit verfolgt?
- Basiert die Speicherung auf einer zulässigen Datenerhebung?
- Ist die Datenspeicherung auf einer gesetzlichen Grundlage zulässig und zur Aufgabenerfüllung erforderlich?
- Wurden die formellen Anforderungen an Datei hinsichtlich Verfahren und Transparenz beachtet?
- Ist die Speicherung des konkreten Datums bzw. Datensatzes verhältnismäßig?
- Ist das gesamte Speicherverfahren (Datei, Datenbank) angemessen und wird dabei der Grundsatz der Datensparsamkeit beachtet?

Bei der Feststellung von Rechtsverstößen bei der Datenspeicherung können sich eine Vielzahl unterschiedlicher Rechtsfolgen ergeben: Löschung, Sperrung, Berichtigung, Zusatzspeicherung, Schadenersatz, Verwertungsverbot.

XV.
Perspektiven

Die technische Entwicklung hinsichtlich Datenerhebung, -speicherung, -auswertung und -übermittlung verläuft rasant. Diese allgemeine Feststellung gilt auch in Bezug auf die personenbezogene Datenverarbeitung der Polizei. Während jedoch die allgemeine Diskussion über die rechtlichen Konsequenzen dieser technischen Entwicklung intensiv geführt wird, trifft dies für die polizeiliche Datenverarbeitung und deren rechtliche und soziale Implikationen nicht (mehr) zu.

Anders als in den 80er und Anfang der 90er Jahre ist die polizeiliche Informatisierung, deren Ausbau und deren Internationalisierung, ein exekutives Spezialthema, das von der öffentlichen Auseinandersetzung nur selten wahrgenommen wird.

Dem entsprechend erfolgt auch nur rudimentär eine anwaltliche Befassung mit polizeilicher Datenspeicherung. Doch auch hierfür gäbe es genügend Anlass. Dieser besteht nicht nur in der Verschärfung des Informationsgefälles im Strafverfahren und in der suggestiven Wirkung von Datenspeicherungen, sondern auch in der rechtlichen Bewältigung dieses Gefälles im Strafverfahren und der Möglichkeit anwaltlicher Verteidigung. So ist z. B. die Frage, inwieweit und unter welchen Umständen sich aus einer unzulässigen Datenspeicherung Beweisverwertungsverbote ergeben, kein Thema für die rechtswissenschaftliche Debatte und auch nicht höchstrichterlich geklärt. Die Digitalisierung des Strafverfahrens harrt noch seiner theoretischen und praktischen Aufarbeitung.

Jenseits der konkreten Strafverfahren hat die polizeiliche Datenspeicherung auch eine hohe gesellschaftliche und politische Relevanz. Die technischen Entwicklungen im Bereich der Informations- und zunehmend stärker auch der Biotechnologie bewirken, dass nicht nur in das Recht auf informationelle Selbstbestimmung, sondern in eine Vielzahl weiterer Grundrechte sowie rechtsstaatliche Verfahrensgarantien – digital – tangiert werden.