Missing Link: Polizeidatenbanken – Datenerfassung im Wirrwarr

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: ronstik/Shutterstock.com) </figcaption></figure> Polizeidatenbanken müssen Datensparsamkeit und Auskunftsersuchen der Politik berücksichtigen. Die vielen Systeme und Schnittstellen sollen konsolidiert werden. Aktuell besteht ein ziemlicher Wirrwarr an Polizeidatenbanken in Bund und Ländern. Das soll sich mit dem Programm „Polizei 2020 [1]“ zwar ändern: Damit sollen die verschiedenen IT-Systeme konsolidiert und an zentraler Stelle einheitliche, moderne Verfahren entwickelt werden. Und alle Polizeien sollen diese dann nach den gleichen Standards nutzen. Aber so weit ist es noch nicht. Wie sieht es jetzt also aus: Was für Datenbanken werden von den deutschen Polizeien genutzt, wer hat auf die Daten Zugriff, wie sieht es mit den gespeicherten Datensätzen aus, wie mit Verknüpfungen unterschiedlicher Datenbanken – und wie mit Datenschutz und Bürgerrechten? „Datenbank“ ist ein weit gefasster Begriff, allein bei der Thüringer Polizei gibt es etwa 200 verschiedene IT-Verfahren, und vielen von ihnen liegt eine Datenbank zugrunde. In diesem Artikel geht es nur um jene Systeme zur elektronischen Datenverwaltung, die Datensätze zu Verdächtigen, Überführten, Verbrechen und Ähnliches enthalten. Sie unterscheiden sich anhand der polizeilichen Arbeitsabläufe, Vorgangsbearbeitungssysteme (VBS), Informationssysteme (Personen- und Sachfahndungen) und Fallbearbeitungssysteme (FBS). Sehr viele Datenbanken basieren auf Produkten von Oracle in der Sprache SQL. Die Polizeien ergänzen sie für ihren spezifischen Bedarf durch Eigenentwicklungen und Zukäufe. Weil die Datenlandschaft des BKA sowie der polizeiliche Verbund seit den 1970er Jahren je nach dem, was die Arbeit forderte und die Technik hergab, aufgebaut und weiterentwickelt werden, wursteln sich die Polizeien heute mit einer Vielzahl unterschiedlicher Datenbanken durch. So ein Durchwursteln ist typisch für große Organisationen und Zusammenhänge. Und nun sind viele Dateien, so das BKA, „kaum miteinander verbunden“. <div class=„collapse-

boxtarget collapse-boxcontent a-inline-textboxcontent a-inline-textboxcontent–horizontal-layout“ data-collapse-target=„“> <figure class=„a-inline-textboximage-container“></figure> Was fehlt: In der rapiden Technikwelt häufig die Zeit, die vielen News und Hintergründe neu zu sortieren. Am Wochenende wollen wir sie uns nehmen, die Seitenwege abseits des Aktuellen verfolgen, andere Blickwinkel probieren und Zwischentöne hörbar machen. <ul class=„a-inline-textboxlist“><li class=„a-inline-textboxitem“>Mehr zum Feuilleton „Missing Link“ [2] mehr anzeigen <h3 class=„subheading“ id=„nav_internationale0“>Internationale, nationale und regionale Ebene</h3> Mehrere internationale Behörden unterhalten Systeme, zu denen deutsche Behörden, vor allem das Bundeskriminalamt (BKA), Verbindungen haben. Die (regional) größte Ausbreitung hat „Automated Search Facility [3]“ als Fahndungssystem für die Mitgliedstaaten von Interpol. Auf EU-Ebene gibt es seit 2005 das Europol-Informationssystem [4] und von eu-LISA [5] das Schengener Informationssystem (SIS) [6], das europäische daktyloskopische System (Eurodac [7]), das Passenger Name Record System und das VISA-Informationssystem [8]. Auf Bundesebene gibt es eine Reihe von Datenbanken, auf die Bundes- und Landespolizeibehörden Zugriff haben. Dazu gehören das Zentrale Verkehrsinformationssystem des Kraftfahrt-Bundesamtes [9] (KBA), das Ausländerzentralregister [10] (AZR) des Bundesverwaltungsamtes, das Bundeszentralregister [11] (BZR) des Bundesamtes für Justiz, außerdem die Fahrzeugdatenauskunft (FADA) der Fahrzeughersteller. Das BKA als Zentralstelle der deutschen Polizei betreibt das „Informationsnetz Polizei [12]“ (INPOL) im Verbund mit den Polizeien des Bundes und der Länder sowie den Zollbehörden, erstellt vom so genannten

Inpol Polas Competence Center (IPCC), nämlich BKA, Länderpolizeien und Zollbehörden. Dabei gibt es den Bundesbestand „INPOL-Zentral“ und einen jeweiligen Landesbestand, etwa INPOL-HH für Hamburg. Daten in INPOL stehen gleich nach der Erfassung allen angeschlossenen Behörden, also auch den Polizeien des Deutschen Bundestag und dem Kraftfahrt-Bundesamt [13] zur Verfügung. Zusätzlich zu diesen Informationssystemen bestehen zudem IT-Systeme für die Telekommunikationsüberwachung sowie das Hinweisportal, eine Art Online-Zeugenaufruf, das aber jeweils freigeschaltet werden muss. Aus dem Jahr 2011 gibt es eine Zusammenstellung der Polizeilichen Datenbanken der Bundesländer [14], die aber nicht vollständig und auch nicht mehr ganz aktuell ist – ebensowenig wie die Gesetzeslage, so ist am 25.05.2018 das neue Bundeskriminalamtgesetz [15] (BKAG) in Kraft getreten. (Auch die folgende Aufzählung ist nicht vollständig. Dafür aber aktualisiert und gewichtet.) Generell können Länderpolizeien auf mehrere Verbunddateien zugreifen, darunter solche mit Zugriff für alle, wie INPOL – mit je einem zusätzlichen eigenen Datenbestand für die Länder –, SIS sowie PIAV. Daneben gibt es Verbunddateien, an denen nur einige Länder teilnehmen wie das VBS @rtus (Bremen, Schleswig-Holstein, Bundespolizei). Zusätzlich haben die einzelnen Länder eigene Anwendungen eingerichtet und erstellen, erfassen und nutzen sie bei Sonderdienststellen Falldateien. <h3 class=„subheading“ id=„nav_datenbanknutzung1“>Datenbanknutzung der unterschiedlichen Landes-Polizeien</h3> Die nidersächsische Polizei zum Beispiel nutzt die Landesanwendungen Nidersächsisches Vorgangsbearbeitungs-, Analyse-, Dokumentations- und Informations-System (NIVADIS [16]), das Polizeiliche Auskunftssystem (POLAS), und das FBS Software zur Analyse, Fallbearbeitung, Informationsverarbeitung und Recherche (Safir). Die Polizei Hamburg nutzt für die Vorgangsbearbeitung und zum Informationsaustausch unter anderem das computergestützte Vorgangsbearbeitungssystem ComVor und die Kriminalakte. Die Polizei Bremen nutzte von 1984 bis 2005 ISA-D und von 2005 bis 2014 ISA-Web, seit dem Jahr 2014 nutzt sie @rtus: Dabei handelt es sich um eine Eigenentwicklung im Auftrag der @rtus-Kooperation der Polizei Schleswig-Holstein, der Polizeien im Land Bremen sowie der Bundespolizei, zusammen mit der Firma Dataport. Zur Fallbearbeitung nutzt sie das FBS Polizeiliche Information, Ermittlung und Recherche (PIER) auf der Basis der Software rsCase der Firma rola Security Solutions GmbH. Die Landespolizei Schleswig-Holstein nutzt das VBS @rtus für die Vorgangsbearbeitung und zum Informationsaustausch, außerdem das FBS Merlin und die Kriminalakte. In Rheinland-Pfalz betreibt die Polizei für die polizeiliche Vorgangsbearbeitung und die Darstellung der Straftatenlage jeweils seit dem Jahr 2002 die Anwendungen POLADIS und POLIS (beide Microsoft), KLAUS und GeopolisK (beides Eigenentwicklungen), und seit 2006 auf der Basis von Oracle KRISTAL (rola Security Solutions GmbH). Die Polizei in Sachsen-Anhalt verfügt über das Informationssystem der Polizei des Landes Sachsen-Anhalt (ILSA), das Integrierte Vorgangsbearbeitungssystem der Polizei (IVOPOL), das Web-Auskunft und -Recherchesystem der Polizei Sachsen-Anhalt (WARSA) und das Elektronische Freiheitsentziehungsbuch (EFB). <h3

class=„subheading“ id=„nav_anforderungen2“>Anforderungen an die Informationen</h3> Die Polizeien müssen mit ihren Datenbanken nicht nur die eigenen Informationen, Fälle und Vorgänge verwalten, sondern sie müssen auch die Belange anderer Behörden berücksichtigen. So gibt der Abteilungsleiter der Serviceeinheit Informations- und Kommunikationstechnik [17] (SE IKT) Oliver Knecht zu bedenken: „Wir reden hier über die polizeilichen Datenbanken oder Datensysteme. Aber man darf nicht außer Acht lassen, dass die Polizei sich auch organisieren und verwalten muss. Und wir nehmen spätestens mit der Umsetzung des Berliner E-Government-Gesetzes auch die Systeme, die uns verwalten, in unseren Bereich herein.“ Viel zu tun, nämlich Finanzsysteme und Personalverwaltungssysteme mit stadtweiter Gültigkeit und große Themen wie die E-Akte oder die Zulieferung polizeilicher Daten an die Justizbehörden. „Dabei handelt es sich um riesige Datenmengen“, erklärt er: „Dazu gehören bestimmte Anforderungen zum Teil unter Berücksichtigung verschiedener rechtlicher Belange. Für uns gelten StPO, StGB, ASOG, bestimmte Verkehrsregelungen. Für unsere „Kunden“, die Justiz, gelten möglicherweise ganz andere Regelungen, dem müssen wir auch nachkommen.“ Die Berliner Polizei nutzt das FBS Computergestützte Anwendung für Sachbearbeitung und Auswertung (CASA), eine Berliner Abwandlung der Software rsCase der Oberhausener Firma rola Security Solutions GmbH. Als Vorgangsbearbeitungssystem (VBS) nutzten die Berliner früher das Informationssystem für Verbrechensbekämpfung (ISVB). Dies wurde im März 2005 abgelöst durch das Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (Poliks), eine modulare IT-Plattform als zentrales VBS. Entwickelt wurde Poliks von der Deutsche Telekom Health and Security Solutions (DTHS) (früher Gedas), einer hundertprozentigen Tochter der Telekom. Es läuft vor allem mit Linux, die Server stehen im IT Dienstleistungszentrum Berlin (ITDZ). Alle Daten, die in Poliks eingegeben werden, können weiter ausgewertet, aufbereitet und verwendet werden. Die Daten werden generiert und – nach einer händischen Qualitätskontrolle, wie bundesweit gewünscht – über eine Schnittstelle in das zentrale PIAV-System eingespielt, auf das alle Bundesländer zugreifen können. Derzeit sitzt die Polizei daran, das System mit weiteren Modulen zu ergänzen, etwa eine elektronische Asservatenverwaltung, die demnächst in Betrieb gehen soll. An Poliks arbeitet eine Projektgruppe von ausschließlich Polizeivollzugsbeamten, die formulieren, was für die Kollegen „draußen“ entwickelt werden soll. Dazu gehören Anforderungsmanagement, Problemmanagement, die Betreuung der Hotline sowie die Abdeckung eines Testbereiches, wenn neue Software-Releases ausgeliefert werden. Das ist nicht immer einfach. Gruppenleiterin von SE IKT C 2 Petra Löffler: „Wir haben eine Dolmetscherfunktion, weil die Entwicklerfirma eine andere Sprache spricht als die Polizei. Wir übersetzen Polizeisprache in IT-Sprache.“ Das ist personalintensiv: „Auf der DTHS-Seite haben wir einen festen Personalstamm, der sich uns auch angenähert hat. Das sind bei uns mit der Hotline 26 Polizeibeamte, und bei der Entwicklerfirma ungefähr 10 bis 12 Berater. Wir betreuen komplett die gesamte 'Poliks-Familie'.“ <h3 class=„subheading“ id=„nav_missbrauch3“>Missbrauch innerhalb der Polizei</h3> Die Rechtsanwältin Seda Başay-Yıldız hatte sowohl die Familie eines Mordopfers im NSU-Prozess als auch islamistische Gefährder vor Gericht vertreten. Dann bekam sie Drohbriefe, unterzeichnet mit NSU 2.0, die sich gegen ihre kleine Tochter richteten und in denen interne Daten aus dem Polizeicomputer standen. Eigentlich haben Polizeibedienstete nur soweit Zugang zu den Dateien, wie sie die gespeicherten Informationen zur rechtmäßigen Erfüllung ihrer Aufgaben benötigen. Abfragen und Eingaben werden im Allgemeinen durch das System protokolliert. Zugriff auf diese Protokolldaten kann beispielsweise ein behördlicher Datenschutzbeauftragter haben. Im Einzelnen gibt es allerdings

unterschiedliche Regularien. Im BKA ist der Zugriff im Wesentlichen durch das BKA-Gesetz (BKAG [18]) geregelt. „Daraus“, so die Pressestelle, „resultieren Berechtigungskonzepte, die die Adressatenkreise identifizierbar machen und den Berechtigten durch sogenannte Administratoren den systemischen Zugang erlauben, versagen oder beschränken. Die Protokollierung erfolgt aufgrund der gesetzlichen Regelungen des BKAG sowie des BDSG. Der Zugriff auf die Protokolldaten erfolgt ausschließlich gemäß den Regelungen des BDSG.“ <h3 class=„subheading“ id=„nav_in_den_ländern4“>In den Ländern gelten weitere Gesetze</h3> In Sachsen-Anhalt zum Beispiel gilt ein Runderlass des MI [19] von 2013: Es wird protokolliert, wer wann welche personenbezogenen Daten in polizeilichen automatisierten Verfahren verarbeitet oder genutzt hat (Revisionsfähigkeit), sprich: Datum und Uhrzeit (von – bis), Terminal- und Benutzerkennung, Art des Dialogs und eingegebene, abgefragte und gelöschte Daten. In Bremen ist eingabe- und abfrageberechtigt, wer mit den Ermittlungen beauftragt ist. Dies gilt für die Bediensteten der Polizei Bremen und der Ortspolizeibehörde Bremerhaven und betrifft ihre Abfragen bei INPOL sowie die Eingaben und Abfragen bei VBS @rtus und FBS PIER. INPOL, VBS @rtus und FBS PIER protokollieren den Zugriff systemseitig und speichern ihn 12 (FBS PIER) bzw. 24 (INPOL, VBS @rtus) Monate lang in der jeweiligen Datenbank; Zugriff auf diese Protokolldaten hat jeweils der behördliche Datenschutzbeauftragte. Auch in Nordrhein-Westfalen wird die Protokollierung der Zugriffe jeweils in den Anwendungen geregelt, die Aufbewahrungszeiten der Protokolldateien sind unterschiedlich und auch abhängig von den jeweiligen Verfahren und ihren Datenspezifika. Maßstab ist insbesondere das Datenschutzgesetz NRW. Bei Verbundanwendungen mit anderen Bundesländern oder dem BKA gelten die jeweiligen Errichtungsanordnungen oder Verfahrensverzeichnisvorschriften. In Rheinland-Pfalz sind die Zugangsberechtigungen auf POLADIS, KLAUS, GeopolisK, sowie zu POLIS in Generalerrichtungsanordnungen (GEA) geregelt, so die Pressestelle: Der Zugriff auf die Daten wird für 12 Monate protokolliert. Der Zugriff auf die Protokolldatei ist nur unter den Voraussetzungen des § 64 Abs. 3 LDSG zulässig. Solch ein Zugriff zur Sicherstellung eines ordnungsgemäßen Betriebs ist beschränkt auf Einzelpersonen des Polizeipräsidiums Einsatz, Logistik und Technik und den örtlich zuständigen Behördlichen Datenschutzbeauftragten. Ein Zugriff zur Datenschutzkontrolle durch die behördlichen Datenschutzbeauftragten ist mit Genehmigung des Ministeriums des Innern und für Sport möglich, sowie durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Auch der Zugriff auf KRISTAL ist in einer GEA geregelt, Zugriff haben spezialisierte Sachbearbeiter der Polizeipräsidien und des Landeskriminalamtes, wenn sie diese Daten für Auswertungen von Ermittlungs- und Strukturverfahren für die Verbrechensbekämpfung benötigen. In Baden-Württemberg erfolgt laut Pressestelle in allen Systemen eine 100 Prozent-Protokollierung zur Datenschutzkontrolle, Datensicherheit, Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und wenn Anhaltspunkte dafür vorliegen, dass ohne ihre Verarbeitung die vorbeugende Bekämpfung oder Verfolgung von Straftaten mit erheblicher Bedeutung (§ 22 Absatz 5 PolG BW) aussichtslos oder wesentlich erschwert wäre. Die Protokolldaten werden für 12 Monate gespeichert und danach automatisiert gelöscht, es sei denn, es liegt zu diesem Zeitpunkt ein Antrag auf Auswertung vor. Ausgewertet werden die Protokolldaten nur auf Antrag des zuständigen Dienststellenleiters oder seines Vertreters im Amt. Der behördliche Datenschutzbeauftragte prüft den Antrag und

entscheidet darüber, bei einem positiven Bescheid wertet der Datenbankadministrator die Protokolldaten aus. <h3 class=„subheading“ id=„nav_zugriffskontroll5“>Zugriffskontrolle und -protokollierung</h3> In Berlin sind die gesetzlichen Vorgaben: Strafprozessordnung und Allgemeine Sicherheits- und Ordnungsgesetz des Landes Berlin (ASOG Bln), in Kombination mit der Verordnung über Prüffristen bei polizeilicher Datenspeicherung. Petra Löffler: „Daraus resultierend gibt es für Poliks mehrere Errichtungsanordnungen, wo auch noch einmal ganz klar vorgegeben wird, wie lange welche Daten aufbewahrt werden dürfen.“ In Berlin ist ein fünfstufiges Lesestufenkonzept eingerichtet. Das reicht von der Sicht auf Grunddaten – Name des Vorganges und Bearbeiter – bis zur Sicht auf den einzelnen Vorgang und die darin enthaltenen personenbezogenen Daten. Die Anzahl der Nutzer pro Abstufung ist nicht festgelegt: Jeder der insgesamt 16.000 Nutzer hat individuelle Rechte, die für einen Vorgang jeweils errechnet werden. Dies sind also jeweils arbeitsbezogene Berechtigungen, und wenn jemand Dienststelle oder Deliktbereich wechselt, dann werden seine Berechtigungen seinem neuen Aufgabenbereich angepasst. Dies alles funktioniert automatisiert, erklärt Petra Löffler: „Sie rufen den Vorgang auf und direkt beim Aufrufen wird das Lesestufenkonzept berechnet. Dann öffnet sich der Vorgang gleich in entsprechender Form.“ Achim Walther, der Referatsleiter von SE IKT C ergänzt: „Das geht sogar so weit, dass man beim Start von Poliks nur die Module sieht, zu denen man berechtigt ist. Es gibt Kollegen, die gar nicht wissen, wie viele Module Poliks hat, weil sie damit nichts zu tun haben.“ <h3 class=„subheading“ id=„nav_datenauswertung6“>Datenauswertung per Knopfdruck</h3> Das Berliner Poliks hat eine weitere Besonderheit gegenüber den VBS anderer Bundesländer: Es hält eine ganze Reihe Pflichtfelder vor, die man ausfüllen muss, sonst kommt man nicht weiter in der Bearbeitung. „Eine zwiespältige Geschichte“, sagt Oliver Knecht, „einerseits gibt es die Kollegen, die zum Teil nachts um drei irgendwo sitzen und mit dem System arbeiten. Andererseits gibt es die Kollegen, die Rede und Antwort stehen müssen, zum Beispiel im Sicherheitsausschuss im Abgeordnetenhaus.“ Und das ist nicht alles: „Außerdem sind bestimmte statistische Fragestellungen entstanden, die deutlich über die reine Bearbeitung der Kriminalität hinausgehen, also wie viele Morde, Raubtaten, Vergewaltigungen es gab. Jetzt wird auch gefragt, wie viele Jugendliche, Opfer, Täter betroffen waren, wie oft eine Waffe, ein Messer benutzt wurde, oder welche Tatmodalitäten eine Rolle spielten.“ Der Punkt ist: „Dadurch, dass wir dieses technische Instrument eines Data Warehouse haben, können wir diese Dinge sofort abbilden, sobald sie in Poliks und in der PKS tatsächlich erfasst werden. Andere Länder können das nicht, jedenfalls nicht so schnell und genau und verlässlich.“ Wie läuft das ab? Petra Löffler: „Der Polizist bearbeitet seinen Vorgang einer Straftat im VBS Poliks. Wenn er fertig ist, dann schließt er den Vorgang ab. Und damit werden alle PKS-relevanten Daten in einen Bereich innerhalb von Poliks eingespeichert, einem Poliks-Plug-in namens PKS. In diesem Plug-in befinden sich jetzt nur diejenigen Teile des eigentlichen Vorgangs, die PKS-relevant sind. Dazu gehören das Delikt, die Anzahl der Tatverdächtigen oder das Alter des Geschädigten: Das, was die PKS braucht. Und auf Basis dieser Daten wird dann das Data Warehouse berechnet. Diese Daten werden täglich in das Data Warehouse exportiert, so dass die statistischen Daten dort auf Knopfdruck aufbereitet werden können.“ Achim Walther ergänzt: „Das Data Warehouse ersetzt das händische Auszählen einzelner Straftaten, die jeweils für die PKS abgefragt werden. Poliks gibt das ins Data Warehouse und generiert daraus die Antworten, die vorher mal im Data Warehouse sozusagen hinterlegt wurden.“ Das hilft der Polizei in der öffentlichen Wahrnehmung. Oliver Knecht: „Denn diese Zahl, wie oft zum Beispiel ein Messer benutzt wurde, steht im Grunddatenbestand von Poliks, und da ziehen wir sie uns raus. Das ist ein Luxus, an den sich viele gewöhnt haben, der aber nicht im bundesweiten Vergleich die Regel ist.“ Für die Berliner ist das hilfreich: „Weil, das muss man auch ganz klar sagen, wir werden hinterfragt. Behördenleitung, Politik: Die Innenverwaltung muss Rede und Antwort stehen. Und

es kommt nicht gut an, wenn im Rahmen verschiedener Anfragen möglicherweise unterschiedliche Zahlen dargestellt werden. Es muss eine verbindliche Zahl geliefert werden, damit nicht der Eindruck entsteht, dass die Polizei im Grunde ihre eigene Arbeit oder ihre Ergebnisse nicht richtig darstellen kann. Aber das haben wir mit Poliks und durch die Verarbeitung der dort gespeicherten Daten im Augenblick ganz gut erreicht.“ Früher war das anders, wenn etwa im Rahmen der Demonstrationen am 1. Mai nach Festnahmen, Verhaftungen etc. gefragt wurde, was bei Behörden unterschiedliche Dinge sind, für Journalisten und Zeitungsleser jedoch nicht unbedingt. Um auf die Drohungen gegen die Anwältin Seda Başay-Yıldız zurückzukommen: Ein Polizist wurde im Rahmen der Ermittlungen festgenommen [20] und am selben Tag wieder freigelassen, da keine Haftgründe vorlagen und ein dringender Tatverdacht nicht nachgewiesen werden konnte. Aber es wird weiter ermittelt. Die Protokollierung von Zugriffen ist scheinbar auch zu umgehen. <h3 class=„subheading“ id=„nav_datensätze7“>Datensätze – was steht drin</h3> Ein Beispiel: Seit den Morgenstunden des 18. Februar 2019 wird Rebecca Reusch vermisst. Die Polizei geht inzwischen davon aus, dass sie getötet wurde, hat aber bislang weder einen Mörder noch eine Leiche gefunden. Im Rahmen der Ermittlungen veröffentlichte sie einen Zeugenaufruf nach einem Auto. Nur ein damals Tatverdächtiger hatte darauf Zugriff, und sein Kennzeichen wurde in Brandenburg vom mobilen Kennzeichenerfassungssystem „KESY“ [21] erfasst. Es wurde außerdem gespeichert und konnte von der Brandenburger Polizei nachträglich abgerufen werden. Im Allgemeinen gibt es gesetzliche Grundlagen für die Erhebung, Speicherung und Löschung von Datensätzen, unter anderem StPO, das BKAG, die Polizeigesetze der Länder, Errichtungsanordnungen etc. Beim BKA unterliegt die Einhaltung der rechtlichen Vorgaben einer Kontrolle, unter anderem des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Beim BKA lagern sehr viele Datensätze, in der INPOL-Personenfahndungsdatei waren am 1. April 2019 genau 305.215 Ausschreibungen zur Festnahme und 394.786 Ausschreibungen zur Aufenthaltsermittlung registriert; in der Sachfahndungsdatei etwa 16.000.000 Gegenstände, die wegen eines möglichen Zusammenhangs mit Straftaten gesucht werden. Die Dauer ihrer Speicherung hängt von der Gesetzeslage ab; es können bis zu zehn Jahre sein. Für so genannte „Kriminalpolizeiliche personenbezogene Sammlungen“ (KpS) geben unter anderem das BKAG, die STPO und die Polizeigesetze der Länder Richtlinien vor. So etwa wird in Bremen dem Bremer Polizeigesetz (BremPolG) [22], entsprechend im VBS @rtus gespeichert, die Speicherung bei INPOL und dem FBS PIER richtet sich außerdem nach der STPO und dem BKAG. Mit Stand 25. Februar 2019 waren im VBS @rtus im Modul „elektronische Kriminalakte“ (eKA) 42.406 Personendatensätze gespeichert, und in INPOL mit Stand 22. Februar 2019 waren 46.582 Bremer personen- und 260.676 Sachdatensätze gespeichert. Im FBS PIER Stand 25. Februar 2019 waren 55.195 Bremer Personen- und 91.207 Bremer Sachdatensätze gespeichert. <h3 class=„subheading“ id=„nav_dauer_und_art8“>Dauer und Art der Informatiosnspeicherung</h3> Manche Datenbanken, so etwa KLAUS und GeopolisK in Rheinland-Pfalz, dienen der Lagedarstellung und enthalten gar keine personenbezogenen Daten, so die Pressestelle. In Rheinland-Pfalz heißt das Landessystem zum Fahndungssystem INPOL POLIS und enthält Daten zu Personen und Sachen, die zur Gefahrenabwehr, vor allem zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Das sind etwa Informationen zu Straftaten einzelner Personen, und ob diese Personen zum Beispiel erkennungsdienstlich behandelt oder zur Fahndung ausgeschrieben sind. Die Erfassung richtet sich nach den DKpS-Richtlinien (Führung Digitaler Kriminalpolizeilicher

personenbezogener Sammlungen und Dateien bei der Polizei Rheinland-Pfalz) und den Rahmenrichtlinien für den Kriminalaktennachweis (KAN) des Bundes. KRISTAL wiederum dient der Sammlung, Auswertung und Zusammenführung von Informationen zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, zur vorbeugenden Bekämpfung und zur Aufklärung von Straftaten insbesondere mit internationaler, länderübergreifender oder erheblicher Bedeutung und ist in der GEA für das Verfahren geregelt. Es gibt Fristen für die Speicherung von Daten in den diesen Systemen, sie sind in den GEA geregelt. Auch in Baden-Württemberg richtet sich die Dauer der Speicherung personenbezogener Daten unter anderem nach dem Polizeigesetz, hier natürlich dem in Baden-Württemberg. Dies unterscheidet nicht nur verschiedene Speicherzwecke wie Dokumentation, Gefahrenabwehr, Störungsbeseitigung, Schutz privater Rechte, vorbeugende Straftatenbekämpfung, sondern auch Personenrollen wie Störer, Zeuge oder Hinweisgeber. Die Speicherdauer wird „nach Gesamtbetrachtung“, so die Pressestelle, im Rahmen der gesetzlichen Vorschriften festgelegt. Dabei wird „systemseitig sicherstellt, dass eine gesetzliche Höchstdauer nicht überschritten werden kann. Unter bestimmten rechtlichen Voraussetzungen kann bei Erreichen der Aussonderungsprüffrist die Speicherung verlängert werden, der Grund dafür muss dokumentiert werden.“ In manchen Ländern erledigt ein Dienstleister die Datenverarbeitung und die Daten liegen dann aber bei einer Polizeibehörde, so läuft es zum Beispiel mit dem LZPD in NRW. Und in Berlin wird das Verfahren Poliks als eines von ganz wenigen Verfahren vom ITDZ gehostet. <h3 class=„subheading“ id=„nav_implementiertes9“>Implementiertes und automatisiertes Fristen- und Löschkonzept</h3> Bei der Berliner Polizei werden die Daten unter dem Dach von Poliks gespeichert. Oliver Knecht: „Wir liefern und empfangen Daten auf Bundesebene. Es gibt einen Datenaustausch zu verschiedenen Dienstbereichen im Rahmen der Tätigkeiten, wenn es denn erforderlich ist. Tatsache ist, dass das Volumen insgesamt sehr groß ist, wir sind eine der größten Länderpolizeien. Wir haben hier in der Regel pro Jahr eine halbe Million Straftaten.“ Petra Löffler: „… Und eine Million Vorgänge in Poliks.“ Und die Löschung? Petra Löffler: „Die grobe Richtung ist, dass wir personenbezogene Daten von Tatverdächtigen entsprechend der Prüffristenverordnung fünf oder zehn Jahre aufbewahren, je nach Schwere des Delikts. Und dann wird es noch mal untergliedert: So gelten unterschiedliche Fristen für Erwachsene, Jugendliche oder Kinder. Das alles ergibt sich aus der Prüffristenverordnung. Das gesamte Fristen- und Löschkonzept basiert auf diesen rechtlichen Grundlagen. Das ist auch implementiert und automatisiert. Für jede Datenbank, für jedes Einzelverfahren, das wir betreiben, gelten rechtliche Grundlagen, und diese sind zwingend in eine Errichtungsanordnung einzuleiten.“ Um auf die Suche nach Rebecca Reusch zurückzukommen: Laut einem Bericht des rbb war die Erfassung des Wagens bloß ein Zufallsfund. In Warschau hatte eine Konferenz stattgefunden, die Anlagen sollten der Terrorabwehr dienen. Bei der Brandenburgischen Polizei war man „stinksauer“, dass die Existenz und Möglichkeiten von KESY öffentlich wurden. – Die Frage ist allerdings, ob im Normalbetrieb die erfassten Kennzeichen, die nicht auf Fahndungslisten stehen, tatsächlich sofort wieder gelöscht werden. <h3 class=„subheading“ id=„nav_verbindungen10“>Verbindungen mit internationalen Polizeibehörden</h3> Zweck und Ziel von PIAV und Polizei 2020 sind unter anderem eine bessere Verfügbarkeit von Daten, die dadurch erreicht werden soll, dass Datenbanken Schnittstellen zu einander haben und man Daten untereinander austauschen kann. Aber das ist natürlich auch jetzt schon möglich. Das BKA ist nicht nur die Zentralstelle der deutschen Polizei, sondern bildet auch die Verbindung zwischen deutschen und internationalen Polizeibehörden. Damit ein nationaler sowie ein internationaler Polizeiverbund funktioniert, sind Schnittstellen für den Datenaustausch und -abgleich vorgesehen, so die Pressestelle: „So werden u.a. beim SIS die entsprechenden deutschen Personen- und Sachfahndungsdaten (INPOL-Verbund) via N.SIS

(Nationales SIS) an die C.SIS (Zentrale SIS) in Straßburg übermittelt und somit den Mitgliedstaaten des SIS zur Verfügung gestellt. Weiterhin werden deutsche Daten entsprechend den gesetzlichen Regelungen für weitere Stellen (u.a. Europol, Interpol, eu-LISA) bereitgestellt, aktualisiert und gemäß den Löschvorgaben wieder gelöscht. Auf nationaler Ebene werden natürlich basierend auf den gesetzlichen Regelungen Daten innerhalb des INPOL-Verbundes, also zwischen den daran beteiligten Stellen, ausgetauscht.“ Auch in den Ländern gibt es jetzt schon zahlreiche Schnittstellen. Zum Beispiel hat das Bremer System @rtus Schnittstellen zu PIER und INPOL Land. Und in Rheinland-Pfalz bestehen aus POLADIS Schnittstellen zu den Anwendungen KLAUS, GeopolisK, POLIS sowie zu KRISTAL. In Niedersachsen hofft man dagegen auf das Programm Polizei 2020. Denn, so die Pressestelle, die unterschiedlichen zentralen und dezentralen Systeme und Datenbanken der Polizeien von Bund und Ländern „sind untereinander häufig nur eingeschränkt kompatibel und nur in Teilen mittels Schnittstellen verbunden. Ein automatisierter Datenaustausch ist somit nur eingeschränkt und unter den jeweiligen rechtlichen Rahmenbedingungen möglich.“ Die Berliner Polizei liefert wie die anderen Länder auch dem BKA zu, auch weil dieses die Schnittstelle zum Europäischen Informationsverbund ist. Nicht nur organisatorisch und rechtlich, sondern auch technisch werden die Systeme um Schnittstellen ergänzt. So wird das System der Berliner Polizei, Poliks, ständig erweitert. Petra Löffler zählt auf: „Ursprünglich sind wir mit einem Auskunftsystem, mit der Vorgangsbearbeitung, einem Rechercheteil und einem Anfragemodul für das Bundeszentralregister gestartet. Das sind einzelne Plug-ins oder Applikationen, die unter dem Dach Poliks zusammengefasst sind. Sie sind inzwischen erweitert worden und es gibt deutlich mehr Module, die zur Poliks-Familie gehören. Wir bedienen zum Beispiel auch die DNA-Datenbank des Bundes aus Poliks heraus mit einem eigenen Plug-in. Und selbstverständlich wird Inpol auch aus Poliks heraus bestückt.“ Die Art der Datenverarbeitung ist modern: „Einmal-Erfassung, und die erforderlichen Daten werden nach Inpol übermittelt. Und genauso auch umgekehrt. Wir sind gehalten, bestimmte Daten voll-parallel zu halten und andere teil-parallel. Fahndungen werden zum Beispiel voll-parallel gehalten, damit auch im Fall einer Unterbrechung der Verbindung zwischen Land und Bund in den einzelnen Ländern gefahndet werden kann oder Flüchtige erkannt werden können.“ Eine Fahndung ist innerhalb von Sekunden bundesweit über den sogenannten Nachrichtenaustausch verteilt, man sieht sie Sekunden später in INPOL. Das ist nicht bei allen Daten so: „Teil-parallel wären zum Beispiel Erkennungsdienstliche Daten. Da haben wir nur den Zugriff auf unsere eigenen ED-Daten, wir haben sozusagen nur sie bei uns im System. Wenn wir da Informationen von anderen Bundesländern haben wollten, müssten wir sie beim BKA anfragen.“ <h3 class=„subheading“ id=„nav_verschärfung11“>Verschärfung der Polizeigesetze</h3> An Polizeidatenbanken wird immer wieder grundsätzliche Kritik geübt, berechtigterweise oder nicht: etwa, weil nach der Einstellung eines Ermittlungsverfahren Daten nicht gelöscht werden [23], weil Einträge auch mal ungerechtfertigt sind – als ein polizeiliches Versehen oder als Zufallsfund [24] –, weil etwas Falsches gespeichert wird oder weil Behörden, und sei es nur aus Personalmangel, nicht immer, wie bei Erwachsenen vorgeschrieben, alle zehn Jahre überprüfen, ob Einträge noch gerechtfertigt und erforderlich sind. Dazu kommt die gesetzliche Lage, die der frühere Richter am Bundesverwaltungsgericht Professor Dr. Kurt Graulich beschreibt: Erst hat der Bund im Jahr 2008 das BKAG zu dem am weitesten entwickelten Polizeigesetz in Deutschland gemacht. „Es ist insbesondere eine Antwort auf die vielfältigen Facetten einer zunehmend digitalisierten Kommunikation eingestellt. Oftmals hat der Bund rechtliche Überwachungsinstitute im Polizeirecht sogar eher normiert als in der Strafprozessordnung

(StPO).“ Und nun ziehen die Länder nach: Viele Polizeigesetze werden aktuell verschärft. Bedenklich an der ganzen Angelegenheit ist der Eindruck, dass die Gesetzesänderungen schärfer sind als notwendig. So hat das Bundesverfassungsgericht (BVerfG) die im BKAG enthaltenen heimlichen Überwachungsbefugnisse in einem Urteil vom 20. April 2016 überprüft und umfangreiche Verstöße gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz festgestellt und viele Nachbesserungen verlangt. Und die Gesetzgebungskompetenz für das Polizeirecht liegt zwar grundsätzlich bei den Ländern, schreibt Graulich, aber der Bund habe seit 2006 eine legislatorische Zuständigkeit zur „Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt“. Und die Überwachungsinstitute können auch auf nicht-terroristische Bedrohungen angewandt werden. Das gilt auch für die nachziehenden Länder: Einen „Sprung in die Alltagskriminalität“, nennt der frühere FDP-Politiker Gerhart Baum im DLF es in Bezug auf das besonders scharfe bayerische Polizeigesetz [25]. <h3 class=„subheading“ id=„nav_kritik_von12“>Kritik von Polizisten</h3> Es sind auch keinesfalls alle Polizisten selbst von allem begeistert. Kritik kommt beispielsweise aus Berlin. Oliver Knecht: „Da ergibt sich manchmal ein Widerspruch. Einerseits sind wir gehalten, unsere Systeme nach Datensparsamkeit auszurichten und immer wieder auf das Einfachste herunterzubrechen, nämlich einmalige Erfassung und mehrfache Nutzung. Andererseits sollen und wollen wir die komplexen Fragestellungen politisch und intern beantworten und steuern.“ Detlef Naumann, Informationssicherheitsverantwortlicher für das LKA Berlin: „Wir haben einen politischen Arm, der berechtigt, also wirklich völlig nachvollziehbar darauf achtet, dass wir als Sicherheitsbehörde nicht mehr Daten erfassen als unbedingt notwendig. Aber die Entwicklung der letzten Jahre, beginnend mit dem NSU-Problem, sehe ich genau umgekehrt. Einzelne Politiker fragen etwas sehr Kritisches ab, um ihre politische Identität irgendwie zu belegen. Das zwingt die Sicherheitsbereiche, diese Fragen auch valide beantwortbar zu machen, sprich diese Daten neu zu verarbeiten oder neu zu erfassen. Dann kritisieren sie aber auch diese Sicherheitsbehörde, dass sie zu viel erfassen. Durch dieses zunehmende Reinregieren und Reinfragen, was hast du denn gemacht, was tust du, was erfasst du, zwingt man diese Behörde zusätzliche Datenbereiche, sprich Module oder Selektiermöglichkeiten, darzustellen. Und das halte ich für einen falschen Weg.“ <h3 class=„subheading“ id=„nav_wir_dürfen13“>Wir dürfen nicht darüber sprechen; außerdem haben wir keine Zeit</h3> Nicht alle Polizeien waren so abwägend; einige waren mehr als zurückhaltend. Die hauptsächlichen Quellen für diesen Artikel waren die Antworten auf einen kleinen Fragenkatalog an die Pressestellen des BKA und der Länderpolizeien; ein Gespräch mit einer Gruppe Polizisten vom Fach in Berlin, die Website von BKA und BMI sowie die Parlamentsdatenbanken des Bundestags und mehrerer Landtage. Keine Antwort kam aus Bayern – bezeichnenderweise dem Land mit einem besonders scharfen Polizeigesetz. Das Niedersächsische Ministerium für Inneres und Sport und das Landeskriminalamt Rheinland-Pfalz (die aber Fragen beantwortet haben) griffen in ihren Antworten auf fast identische Textbausteine zurück. Vor allem kamen von den östlichen Bundesländern sowie dem Saarland durchweg kurze und wenig informative Antworten. (Immerhin verlinkten Mecklenburg-Vorpommern, Sachsen und Sachsen-Anhalt auf die Parlamentsdatenbanken der jeweiligen Landtage mit Drucksachen zum Thema.) Die Antworten lauteten sinngemäß: Wir halten uns an die Gesetze und speichern nur, was unbedingt notwendig ist; wir dürfen nicht darüber sprechen; außerdem haben wir keine Zeit. Man kann vermuten, dass der Schutz von Bürgerrechten und Daten mit einer offenen Polizeibehörde Hand in Hand geht. Die Abwägung von Freiheit und Sicherheit wird immer schwierig bleiben. Und der aktuelle Zustand der polizeilichen IT-Systeme ist sicherlich

überholungsbedürftig. Aber diese Systeme und vor allem die aktuelle Tendenz, die Polizeigesetze zu verschärfen, bedarf einer aufmerksamen Beobachtung. Damit der Bürger seine Rechte unbeschadet behält, kann er Auskunftsersuchen stellen, etwa über das Netzwerk Recherche. Er kann klagen. Und er kann Institutionen unterstützen, die den Rechtsstaat kritisch begleiten, etwa Medien, Parteien, Gewerkschaften, Kirchen. ()<br class=„clear“/> <hr/> URL dieses Artikels:
<small>

```
http://www.heise.de/-4469381
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong>&amp;#160;https://www.bmi.bund.de/DE/themen/sicherheit/nationale-und-internationale-zusammenarbeit/polizei-2020/polizei-2020-node.html
```

</small>
<small>

```
<strong>[2]</strong>&amp;#160;https://www.heise.de/thema/Missing-Link
```

</small>
<small>

```
<strong>[3]</strong>&amp;#160;https://interpolnoticeremoval.com/tag/interpol-automated-search-facility/
```

</small>
<small>

```
<strong>[4]</strong>&amp;#160;https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
```

</small>
<small>

```
<strong>[5]</strong>&amp;#160;https://europa.eu/european-union/about-eu/agencies/eu-lisa_de
```

</small>
<small>

```
<strong>[6]</strong>&amp;#160;https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_de
```

</small>
<small>

```
<strong>[7]</strong>&amp;#160;https://edps.europa.eu/data-protection/european-it-systems/eurodac_de
```

</small>
<small>

```
<strong>[8]</strong>&amp;#160;https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_de
```

</small>
<small>

[9] https://www.kba.de/DE/ZentraleRegister/zentralegister_node.html

</small>
<small>

[10] https://www.bva.bund.de/DE/Das-BVA/Aufgaben/A/Auslaenderzentralregister/azr_node.html

</small>
<small>

[11] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/BZR/Inhalt/Uebersicht_node.html

</small>
<small>

[12] https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html

</small>
<small>

[13] https://www.bmi.bund.de/DE/themen/sicherheit/nationale-und-internationale-zusammenarbeit/polizeiliches-informationswesen/polizeiliches-informationswesen-node.html

</small>
<small>

[14] https://www.bundestag.de/resource/blob/412402/f9747432342012e51606e42e5b726072/wd-3-153-11-pdf-data.pdf

</small>
<small>

[15] https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/180525_BKAGneu.html

</small>
<small>

[16] https://www.mi.niedersachsen.de/themen/innere_sicherheit/polizei/technik_und_finanzen/nivadis/nivadis-62624.html

</small>
<small>

[17] https://www.berlin.de/polizei/dienststellen/polizeipraesidium/serviceeinheit-informations-und-kommunikationstechnik/

</small>
<small>

[18] https://www.bka.de/DE/DasBKA/GesetzlicherAuftrag/

```
gesetzlicherauftrag_node.html#doc20666bodyText2
```

</small>
<small>

```
<strong>[19]</strong> http://www.landesrecht.sachsen-anhalt.de/jportal/?quelle=jlink&amp;psml=bssahprod.psml&amp;feed=bssah-vv&amp;docid=VVST-VVST000008781
```

</small>
<small>

```
<strong>[20]</strong> https://www.zeit.de/news/2019-06/27/polizist-nach-drohfax-an-anwaeltin-voruebergehend-festgenommen-190627-99-818836
```

</small>
<small>

```
<strong>[21]</strong> https://www.heise.de/meldung/Klage-gegen-Kennzeichnenscanner-in-Brandenburg-4445598.html
```

</small>
<small>

```
<strong>[22]</strong> http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=168683%2C1
```

</small>
<small>

```
<strong>[23]</strong> https://www.boorberg.de/polizei/Rechtsprechung/Keine+L&amp;ouml%3Bschung+im+polizeilichen+Auskunftssystem+POLAS_4939
```

</small>
<small>

```
<strong>[24]</strong> https://www.heise.de/meldung/33C3-Rechtsexperte-raet-zur-Einsicht-in-Polizeidatenbanken-3582900.html
```

</small>
<small>

```
<strong>[25]</strong> https://www.heise.de/meldung/Experten-kritisieren-massiv-geplante-bayerische-Polizeirechtsreform-4001651.html
```

</small>
<small>

```
<strong>[26]</strong> mailto:bme@heise.de
```

</small>
 Copyright © 2019 Heise Medien </html>