

BULLETIN DER BUNDESREGIERUNG

Nr. 136-4 vom 17. November 2016

Rede des Bundesministers des Innern, Dr. Thomas de Maizière,

auf der Herbsttagung des Bundeskriminalamtes
am 16. November 2016 in Mainz:

„Polizei 2020“

Ich beginne meine Reden von Zeit zu Zeit mit einer Zeitungsmeldung, die mich beschäftigt hat. Und so will ich das – in gewisser Weise – auch heute tun.

Heute gibt es aber eine Besonderheit. Denn heute beginne ich mit Meldungen, die so noch nicht in der Zeitung gestanden haben. Meldungen, die es noch nicht gibt. Ich lese Ihnen einige vor:

„Die Polizei fasst möglichen Attentäter – durch Abgleich im Fingerabdruck-System Eurodac.“

„Erneuter Schlag gegen Organisierte Kriminalität – das europäische Kerndatensystem wirkt.“

„Vernetzte Sicherheit in Bund und Ländern – der neue Informationsverbund steht.“

„Straftaten im Internet – Entdeckungsrisiko so hoch wie niemals zuvor.“

Oder: „Mammutprojekt erfolgreich – BKA-IT grundlegend modernisiert.“

Diese Meldungen könnten so oder so ähnlich in den nächsten Jahren in der Zeitung oder an anderer Stelle zu lesen sein. Und ich möchte solche Meldungen innerhalb der nächsten Jahre lesen – das ist mein Ziel.

Es scheint neuerdings eine gewisse Tradition zu haben, eine sogenannte Agenda über sehr lange Zeiträume zu formulieren. Je länger, desto schillernder. Und so weit weg, dass die Handelnden ganz sicher nicht mehr dabei sind. Dieser Versuchung widerstehe ich.

Ich will heute über die Arbeit der Polizei innerhalb der nächsten vier Jahre sprechen – über die Polizei bis zum Jahr 2020. Manches von dem, über das ich gleich sprechen werde, wird möglicherweise doch etwas länger dauern, als wir es uns wünschen. Aber das befreit uns nicht davon, uns Ziele zu setzen.

Ich beginne für den Blick in die Zukunft mit einem Blick zurück. Ich beginne mit einem Blick auf den 1. September 1971. An diesem Tag wurde Horst Herold zum fünften BKA-Präsidenten ernannt. Innenminister war Hans-Dietrich Genscher – das BKA so etwas wie ein riesiger Zettelkasten.

- Es dauerte vier bis sechs Wochen, bis ein zur Fahndung ausgeschriebener Täter im „Deutschen Fahndungsbuch“ unter der Überschrift „Festnahme“ stand.
- Es dauerte bis zu sechs Monate, bis eine zur „Aufenthaltsermittlung“ ausgeschriebene Person allen Polizeidienststellen mitgeteilt wurde.

In einem Sofortprogramm, das Hans-Dietrich Genscher 1970 dem Bundestag vorstellte, setzte er auf elektronische Datenverarbeitung – abgekürzt EDV. Er gab den Auftrag zur Entwicklung eines gesamtpolizeilichen Systems des Nachrichten- und Informationsaustauschs. Zwischen 1969 und 1973 wurde der Etat des BKA mehr als verfünffacht – von gut 22 auf 122 Millionen D-Mark. Genscher hatte eine Vision der Polizeiarbeit der Zukunft.

Ich zitiere:

„Da steht ein Freund und Helfer mit Walkie-Talkie an der Autobahn und gibt pausenlos Kennzeichen durch. Wenn ein Auto gestohlen ist, kommt aus Wiesbaden prompt Alarm.“

Heute sprechen wir nicht mehr über das Walkie-Talkie an der Autobahn, sondern über Kennzeichenlesesysteme – ich komme darauf zurück.

Genscher ordnete den Einstieg des BKA in das IT-Zeitalter an. In den meisten Bundesländern hatte er schon längst begonnen. Die Länder waren damals schneller als der Bund. Und auch Horst Herold hatte sich vor seinem Einstieg beim BKA in einem Bundesland – in Bayern – seine Meriten erworben.

Schon in den 60er Jahren hatte er in Nürnberg eine EDV aufgebaut, mit der er anhand aktueller Kriminalitätsdaten Einsatzpläne für den nächsten Tag erstellte. Heute nennen wir das staunend „Predictive Policing“.

Das „gesamtpolizeiliche Informationssystem“ – später INPOL genannt – wurde beim BKA in eine Landschaft von IT-Inseln hineinentwickelt. Und dieser Umstand wirkt bis heute nach – das muss man wissen, um die Probleme von heute zu verstehen.

Die damalige Entwicklung geschah in Rekordzeit. Die ersten Stufen von INPOL wurden 1972 eingeführt, zunächst mit der computergestützten Personenfahndung. INPOL wurde ein Riesenerfolg. Der Informationsaustausch der Polizei wurde schlagartig besser. Von Wochen und Monaten hin zu Sekunden, um etwas zu erfahren. Kommissar Computer revolutionierte die Polizeiarbeit in Deutschland.

INPOL war so erfolgreich, dass es stetig gepflegt und weiterentwickelt wurde. Das erste System wurde nach etwa zehn Jahren modernisiert. Die jetzige Version läuft nun seit 2003. Das ist vier Jahre vor Erscheinen der ersten Smartphones, wie wir sie heute kennen – Weiterentwicklungen eingeschlossen.

Die Polizei steht heute vor anderen Herausforderungen als vor 13 Jahren oder zu Zeiten von Horst Herold, aber letztlich stehen wir vor der gleichen Frage: Wie soll unsere

Polizei heute und in den nächsten Jahren arbeiten, um Straftaten zu verhindern, Straftaten aufzuklären und Straftäter zu ermitteln.

Ich will heute über *fünf* Elemente einer „Polizei des Jahres 2020“ sprechen. Diese Elemente sind sicher nicht abschließend, aber wichtig. Sie sind Teil einer Vision und zugleich Hausaufgaben für uns alle.

Das *erste* Element lautet BKA 2020.

Sie alle hier stehen in den Fußstapfen von Horst Herold – und natürlich seinen Nachfolgern. Das BKA muss auch weltweit weiterhin zur Spitze gehören, und zwar in allen Bereichen:

Wir wollen herausragendes polizeiliches Können, wir wollen modernste IT beim BKA und gut ausgebildete Polizisten sollen IT klug und rechtsstaatsicher nutzen.

Wir haben jetzt mit den Sicherheitspaketen im Haushalt 2017 und den damit verbundenen politischen Einigungen die Grundlagen dafür geschaffen, die Sicherheitsbehörden besser auszustatten – dazu zählt natürlich auch das BKA.

Von 2015 bis 2020 wird das Bundeskriminalamt über 1.300 zusätzliche Stellen erhalten. Die Bundespolizei wird – ihrer Personalstärke entsprechend – in diesem Zeitraum um rund 7.500 Stellen anwachsen.

Auch finanziell werden wir das BKA ganz erheblich aufrüsten; so wird der Etat des BKA von knapp 430 Millionen Euro im Jahr 2015 auf rund 574 Millionen Euro im Jahr 2017 und damit um rund 144 Millionen Euro erhöht.

Diese Aufwüchse wollen wir in der Finanzplanung bis 2020 festschreiben, um mit den Entwicklungen Schritt zu halten und auf der Höhe der Zeit zu bleiben.

Jetzt liegt unser Fokus darauf, diese Mittel klug zu investieren. Wir werden die IT-Infrastruktur verbessern – also moderne IT und vor allem modernste Prozesse, auf denen

diese IT dann aufbaut. Kurz: Wir wollen eine neue, moderne IT-Architektur für das BKA.

Wir werden die IT-Landschaft im BKA umbauen – von einer Struktur gut gepflegter, aber verschiedener Datentöpfe zu einer hochmodernen und einheitlichen IT-Architektur.

Und wenn wir über diese neue IT-Architektur der Polizei sprechen, dann hat das auch mit den Anforderungen des Bundesverfassungsgerichts zu tun. Das Bundesverfassungsgericht hat in seiner Entscheidung zum BKA-Gesetz seine Rechtsprechung zum Datenschutz und zur Zweckbindung weiterentwickelt – eine Entscheidung, die wir voll umsetzen und auf die gesamte IT des BKA anwenden werden.

Worum geht es dabei?

Im Mittelpunkt steht der sprachlich etwas sperrige Grundsatz der „hypothetischen Datenerhebung“. Es hat eine Weile gedauert, bis ich das meiner amerikanischen Kollegin Loretta Lynch verständlich erläutern konnte.

Dabei geht es im Kern darum, dass die Eingriffstiefe der jeweiligen Datenerhebungsmaßnahme, zum Beispiel eine Telekommunikationsüberwachung, bei der weiteren Verwendung der Daten streng beachtet wird. Herr Vizepräsident Kirchhof ist morgen hier und wird Ihnen dieses Prinzip bei Bedarf im Einzelnen erläutern.

Wie immer man zu dem Urteil steht. Wir nutzen jetzt das Gesamtkonzept des Bundesverfassungsgerichts, um Polizei-IT und Datenschutz zu verbessern. Die technische Umsetzung dieses Grundsatzes ist aber im Rahmen der bestehenden „Datentöpfe“-IT mit statischen Berechtigungskonzepten nicht oder nicht mit vertretbarem Aufwand möglich.

Theoretisch könnten wir jetzt – mit ein paar Änderungen – die bisherigen Systeme beibehalten. Das wäre der einfache Weg. Wir könnten auf Karlsruhe zeigen, schwächer sein als vorher, mit den Schultern zucken und sagen: Ist halt so.

Damit würden wir aber unserer Verantwortung nicht gerecht. Stattdessen sollten wir uns zutrauen, die gesamte IT umzubauen und die Möglichkeiten, die uns das Bundesverfassungsgericht gegeben hat sowie die Grenzen, die es der Arbeit auferlegt hat, klug zu verbinden in einer IT-Architektur.

Das erfordert etwas Mut und viel Arbeit. Denn mit der gegenwärtigen „Datentöpfe-IT“ können die neuen Möglichkeiten nicht umgesetzt werden. Dafür ist das System nicht nur zu alt, sondern es ist darauf einfach nicht ausgerichtet. Wir bräuchten hunderte von Änderungen in INPOL. Gegenwärtig schaffen wir drei bis fünf Änderungen pro Jahr.

Deswegen machen wir es anders. Wir werden die Anforderungen des Bundesverfassungsgerichts voll umsetzen. Wir werden ein neues BKA-Gesetz schaffen. Und wir werden ein Projekt für die Modernisierung des Informationsmanagements der deutschen Polizei anstoßen.

Und ein Startpunkt dafür ist heute. Das wird sicher ein etwas längerer Weg, der nicht heute beginnt und auch nicht morgen abgeschlossen sein wird. Aber viele Meilensteine sind in den nächsten Jahren erreichbar. Welche Meilensteine das bis wann sind, darüber müssen wir miteinander sprechen und uns gemeinsam auf Ziele einigen.

Ein anderes IT-Großprojekt, das das BKA betrifft, ist ein Fluggastdaten-Informationssystem. Wir werden ein solches System bis Mitte 2018 nach Brüsseler Vorgaben aufbauen. Die europäische Richtlinie ist – endlich – geltendes Recht. Deutschland muss und wird sie fristgerecht in deutsches Recht und in gute Praxis umsetzen.

Die sogenannten PNR-Daten liefern den Sicherheitsbehörden wichtige Hinweise, um Straftäter bei Terrorismus und organisierter Kriminalität aufzuspüren und verdächtige Reisemuster festzustellen. Wir wollen Terroristen erkennen, wenn sie versuchen, durch Europa zu reisen. Wir wollen gefährliche Personen finden, wenn Sie untertauchen wollen. Und wir wollen den Sicherheitsbehörden dafür auch die notwendigen Instrumente an die Hand geben. Ein wichtiges Instrument dafür ist das neue europäische Fluggastdaten-Informationssystem.

Der eigentliche Grund für die erforderliche IT-Modernisierung ist aber natürlich nicht nur die IT allein oder die Verbesserungen, die der Austausch von Informationen bringt. Das tiefere Motiv sind natürlich auch die neuen Wege der Kriminalität und neue Wege, diese Kriminalität zu bekämpfen.

Eigentlich war es schon immer so, dass auch Kriminelle neue Technologien genutzt haben, um Straftaten zu begehen oder sich der Strafverfolgung zu entziehen. Dies gilt heute besonders für den Cyberraum. Das Internet bietet jedem Chancen und Möglichkeiten, aber es wird natürlich auch zur Verabredung und zur Begehung schwerer Straftaten genutzt. Das sogenannte Darknet bietet kriminelle Dienstleistungen wie in einem anonymen Online-Shop zur Bestellung an. Es ist schwierig und aufwändig, hier zu ermitteln – aber nicht aussichtslos. Das zeigen uns erfolgreiche Ermittlungsverfahren des BKA gegen Betreiber von Darknet-Plattformen.

Die Sicherheitsbehörden haben aber auch immer mehr Schwierigkeiten bei Maßnahmen, die früher einfacher Standard waren: Es war zum Beispiel technisch relativ einfach, ein Telefonat von einem Festnetz oder einem einfachen Handy abzuhören – richterliche Beschlüsse et cetera natürlich vorausgesetzt.

Heute steht die Polizei rein technisch vielfach vor komplizierten Aufgaben, wenn die Betroffenen verschlüsselt über Messenger- oder Telefonie-Dienste kommunizieren. Wenn wir hier als Rechtsstaat Schritt halten wollen und Sicherheitsbehörden auch morgen technisch das können sollen, was sie gestern tun konnten, dann müssen wir nicht nur rechtlich auf der Höhe des IT-Zeitalters bleiben.

Kriminalitätsbekämpfung im Internet braucht nicht mehr Rechte für Sicherheitsbehörden als außerhalb des Internets, aber auch nicht weniger. Die Sicherheitsbehörden müssen im Internet auch tatsächlich das technisch können, was sie rechtlich dürfen. Wir müssen bei der Entwicklung von IT-gestützten Ermittlungsmaßnahmen unsere Kräfte bündeln – technische Hilfsmittel entwickeln und auf dem neuesten Stand halten. Jede Behörde kann das nicht für sich. Das gilt zum Beispiel für Entwicklung von Werkzeugen für die Quellen-TKÜ oder die Auswertung von riesigen Datenmengen aus sichergestellten Asservaten.

Ich habe deshalb entschieden, dass wir unser technisches Know-how bei den Sicherheitsbehörden in einer neuen Einrichtung konzentrieren. Diese „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ – kurz ZITiS – wird das BKA und andere Sicherheitsbehörden mit Forschung und Entwicklung unterstützen, um den gegenwärtigen und künftigen Herausforderungen im Cyberraum zu begegnen.

ZITiS beginnt die Arbeit im Januar. Die Befugnisse der Sicherheitsbehörden bleiben bestehen und werden durch die Einrichtung von ZITiS nicht verändert. ZITiS soll die zentrale Stelle für Forschungs- und Entwicklungsaufgaben mit Cyberbezug werden und mit Methoden, Produkten und Strategien die tägliche und operative Arbeit der Sicherheitsbehörden erleichtern. Ich bin sicher: Sie wird allen eine Hilfe sein.

Das *zweite* Element: Bund-Länder Kooperation.

Die aktuelle Situation kann ich – zumindest technisch – in einem Satz zusammenfassen: Wir haben im Moment viele Dateien, aber keinen zentralen Überblick über alle relevanten Erkenntnisse aus Bund und Ländern. Das wollen und müssen wir ändern.

Das hat natürlich auch mit dem BKA und meinem *ersten* Punkt zu tun. Denn das derzeit größte IT-Projekt PIAV leistet hierfür wichtige Vorarbeiten und wird ein zentraler Baustein im angestrebten Informationsverbund sein.

Mit meinen Länderkollegen will ich in zwei Wochen in der IMK Leitlinien diskutieren, an denen wir uns dabei orientieren können. Sie wurden in den Ländern und mit Ihnen erarbeitet. Die Länder sind die zentralen Kooperationspartner – und aus nur technischer Sicht „Kunden“ – des BKA. Die neue IT-Architektur, die das BKA den Ländern zentral zur Verfügung stellen wird, wird sich maßgeblich an den Erfordernissen seiner „Kunden“ ausrichten.

Bei der Gestaltung werden die Länder daher eine entscheidende Rolle spielen. Beim Betrieb und auch bei den Kosten ist der Bund bereit, künftig noch mehr Verantwortung zu übernehmen. Wir wollen bestimmte Dienste, wie etwa auch ein einheitliches Fallbearbeitungssystem, den Ländern künftig kostenneutral zur Verfügung stellen. Auch das wird die IT-Zusammenarbeit zwischen Bund und Ländern nachhaltig verbessern.

Ein weiterer Punkt zur Bund-Länder Zusammenarbeit, nämlich der Punkt Schnittstellen, ist letztlich das Kernproblem von IT-Kooperation – im Bund, zwischen Bund und Ländern und zwischen den Ländern.

Wir hatten im vergangenen Jahr zunächst erhebliche Probleme bei der Registrierung von Flüchtlingen und dem Informationsaustausch der unterschiedlichen Behörden – innerhalb der Bundesbehörden – BKA, BAMF, BPOL, BVA – und mit den Landesbehörden. Daten mussten mehrfach erfasst werden. Registrierte Daten zum Teil ausgedruckt und per Fax weiter übermittelt, weil Schnittstellen zwischen den Behörden entweder fehlten oder die IT-Systeme nicht kompatibel waren.

Wir haben im letzten Jahr hier Einiges gelernt. Aber wir haben auch unsere Schlüsse daraus gezogen. Und wir haben gehandelt. Schneller als bei jedem IT-Projekt früher. Vermutlich war das nur wegen der Krise möglich.

Wir haben den Informationsaustausch und die Arbeitsprozesse zwischen den Behörden optimiert. Wir haben ein Kerndatensystem geschaffen, dessen Rückgrat Fingerabdruckdaten zur eindeutigen Personenidentifizierung bilden. Das ist wichtig, weil die biometrischen Daten häufig die einzigen „objektiven“ Daten sind. Namen und alle anderen Angaben, die die Personen selbst machen, lassen sich leicht variieren oder können fehlerhaft aufgenommen werden.

Jetzt gilt der Grundsatz: Einer für alle bei der Registrierung, jeder für sich bei der Nutzung. Dieser Gedanke – der Gedanke eines Kerndatensystems kann auch als Vorbild eines neuen Informationssystems der Polizei genutzt werden. Denn in seiner Grundarchitektur basiert auch die gesamtdeutsche Polizei-IT bisher darauf, Daten in verschiedenen „Töpfen“ abzulegen.

Den Polizisten wird letztlich nur der Zugriff auf einzelne Töpfe ermöglicht. Zuweilen werden die Töpfe miteinander verbunden, was jedoch eher selten der Fall und technisch immer wieder kompliziert ist. Man könnte sagen: „Viele Töpfe verderben den Brei“ – sie duplizieren Daten unnötig und bergen das hohe Risiko inkonsistenter, unvollständiger und unrichtiger Daten.

Diese Erfahrung machen wir auf der EU-Ebene genauso wie national bei unserer Polizei. Bei Europol ist man deshalb mit der neuen Verordnung, die dieses Jahr in Kraft getreten ist und ab 1. Mai 2017 gilt, neue Wege gegangen. Man hat sich für ein einheitliches Informationssystem entschieden, dem nicht mehr eine Vielzahl von Einzeldateien, sondern auf eine einheitliche analysefähige Plattform zugrunde liegt.

Das ist – finde ich – auch ein Vorbild für die Zusammenarbeit im Bund, zwischen den Ländern und zwischen Bund und Ländern.

Und das führt mich zum *dritten* Element: Europa.

Ich beginne mit einem Beispiel: Der sogenannte „Recklinghausen-Attentäter“ war in ganz Europa mehrfach und unter jeweils anderen Namen registriert. Das ist schlimm genug. Noch schlimmer ist, dass das nicht erkannt wurde, obwohl alle Daten in Europa vorhanden waren und seine Fingerabdrücke mehrfach erhoben wurden.

Das Fingerabdruck-System Eurodac zeigt zwar an, wenn derselbe Fingerabdruck schon einmal in einem anderen EU-Mitgliedstaat gespeichert wurde. Es zeigt aber nicht an, unter welchem Namen der Fingerabdruck gespeichert wurde. Eurodac erfasst diese Information nicht einmal. Das ist Folge eines – gut gemeinten, aber eben schlecht gemachten – Datenschutzes.

Der besteht nämlich auch in der EU gegenwärtig darin, dass etliche Datentöpfe nebeneinander für jeweils gesonderte Aufgaben aufgebaut wurden – ähnlich dem, wie ich es gerade für Deutschland beschrieben habe.

Die europäischen Datentöpfe dienen zwar mehreren, übrigens ähnlich gelagerten Zwecken. Darunter ist meist auch die Strafverfolgung. Aber die Nutzung zu diesem Zweck ist vielfach bis zur Unbrauchbarkeit für die polizeiliche Praxis eingeschränkt, rechtlich und technisch.

In Europa ist es wie in Deutschland: Die vielen unterschiedlichen Datentöpfe sind nicht miteinander verbunden, so dass weder unrichtige Daten noch Zusammenhänge zwischen Daten in verschiedenen Töpfen auffallen. Dies passiert allenfalls zufällig, nicht aber systematisch. So kann es heute eben sein, dass wir die Fingerabdrücke bei Eurodac nur speichern, um zu erkennen, ob eine Person mit denselben Fingerabdrücken in einem anderen Mitgliedstaat bereits einen Asylantrag gestellt hat. Mehr erfährt die Polizei, aber auch die Asylbehörde nicht – nicht einmal den Namen, den der Betroffene beim Asylantrag im anderen Mitgliedstaat angegeben hat. Und ich finde: Das kann nicht sein.

Wir mussten in diesem und im letzten Jahr bitter erfahren, dass die Gefahren des Terrorismus in Europa real sind. Die Lehren, die wir aus den bisherigen Ereignissen in Deutschland und Europa ziehen können, sind im Kern immer wieder die gleichen.

Es sind die gleichen wie beim NSU:

Wir müssen uns überall vernetzen. Ob nationaler oder internationaler, ob politisch oder religiös motivierter Terrorismus – wir können ihm nur begegnen, wenn sich die Sicherheitsbehörden auf einen reibungslosen Informationsaustausch zwischen allen geeigneten und erforderlichen Behörden und Partnern verlassen können. Wenn es nicht gelingt, einer Person schnell anhand vorhandener Informationen nachzuweisen, dass sie falsche Identitäten nutzt, dann ist das ein Fehler in unserer Informationsarchitektur, den alle so schnell wie möglich beseitigen müssen.

Dieses Problem ist nicht neu. Ich habe deshalb – übrigens einen Tag vor den schrecklichen Anschlägen in Brüssel vor acht Monaten – eine Initiative gestartet, die auf ein EU-weites Kerndatensystem zielt.

Statt Fingerabdrücke und die dazugehörigen Personaldaten in Systemen wie Eurodac, dem Schengener Informationssystem, dem VISA-Informationssystem und künftig im Europäischen Einreise-/Ausreisesystem – EES – und Europäisches Reiseinformations- und Genehmigungssystem – ETIAS – getrennt zu speichern, soll dies einheitlich oder mit wechselseitiger Nutzungsmöglichkeit geschehen – mit Zweckbindungen die genau zu regeln sind.

Die Kommission hat den Vorschlag aufgegriffen und erörtert ihn nun mit den Mitgliedstaaten. Ich werde mich dafür einsetzen, dass er so schnell wie möglich umgesetzt wird.

Ich komme zu meinem *vierten* Element und das lautet: Recht und hier insbesondere der Datenschutz.

Wir brauchen ein modernes Recht, das die Chancen der neuen Technik nutzbar macht – genauso wie einen moderneren und einen guten Datenschutz.

Wenn ich als Bundesinnenminister von modernem Datenschutz spreche, dann werden natürlich Fragen gestellt: Geht es darum „alles in einen Topf“ zu werfen? Oder bedeutet die neue IT-Architektur eine Abkehr vom Datenschutz?

Die Antwort darauf lautet: „Nein“. Recht darf Technik nicht konservieren. Und das kann Recht auch nicht.

Einige sagen: Nur die historisch gewachsenen IT-Strukturen können einen guten Datenschutz gewährleisten. Diese Skepsis vor der Technik hat es schon immer gegeben. Und diese Skepsis war in ihrer Pauschalität schon immer falsch.

In den 1920er Jahren haben US-Gerichte ernsthaft erwogen, Autos zu verbieten, weil Kriminelle damit schneller fliehen konnten. Die Polizei verfügte zu diesem Zeitpunkt nicht flächendeckend über Autos. Am Ende haben sich diejenigen durchgesetzt, die auch der Polizei Autos gekauft haben – zum Glück.

Auch der Datenschutz muss sich weiter entwickeln. Er muss technischen Entwicklungen Raum lassen, bei gleichem Schutzzweck. Und er muss diesen Raum auch für sich selbst nutzen. Die Technik bietet hier neue, sogar bessere Möglichkeiten als früher.

Wie könnte ein auf die Zukunft ausgerichteter horizontaler Datenschutz aussehen? Darüber können und müssen wir miteinander diskutieren. Aber ich denke, er bräuchte ein

- geordnetes Zugriffsmanagement,
- Vollprotokollierungen mit Analysefunktionen für die Datenschutzaufsicht und
- ein Datenmanagement, das sich an der Qualität der Eingriffe bei der Datenerhebung orientiert.

Schutz der gesammelten Daten vor unberechtigtem Zugriff und nicht Schutz der getrennten Datentöpfe, das ist effektiver und moderner Datenschutz. Die neue Technik ist auch eine Chance für das Recht – auch für den Datenschutz. Das gilt auch und vor allem bei der Bekämpfung von Kriminalität und Terrorismus in den nächsten Jahren.

Meine Bitte an die Skeptiker ist:

Verlassen wir die alten Schützengräben. Verlassen wir die Konfliktlinien der 70er und 80er Jahre. Öffnen wir uns für die Chancen der neuen, digitalen Möglichkeiten – mit einem Recht, das die Chancen, die sich dort bieten, sieht und nutzt.

Das *fünfte* und letzte Element der Polizei im Jahr 2020 wird Sie vielleicht etwas überraschen, weil es den Fokus gar nicht so sehr auf die Polizei selbst legt. Es lautet: Polizei und Gesellschaft.

Und jetzt spreche ich zunächst mal vom BKA. Denn wie ist denn das Bild eines BKA-Beamten oder vielleicht noch eines LKA-Beamten in der Öffentlichkeit?

Im Alltag haben die Menschen in unserem Land wenig mit dem BKA oder einem LKA zu tun. Sie begegnen öfter einem Streifenpolizisten. Das Bild von BKA und LKA ist dadurch wenig durch eigene Erfahrungen geprägt, sondern vielleicht mehr durch die Darstellung im Fernsehen und anderen Medien.

Und wie ist es denn da?

In vielen Krimis mischt sich das LKA oder das BKA in die Ermittlungen vor Ort ein und wirkt eher störend oder zumindest unsympathisch. Die Einmischung der höheren Instanz ist dem jeweiligen Ermittler in der Regel unwillkommen und wird meist durch eine möglichst unsympathisch wirkende Figur personifiziert. Der Beamte des BKA holt dann seinen Laptop raus und tippt dort griesgrämig irgendetwas ein. Dieses Bild deckt sich weder mit dem Ruf, den das BKA bei seinen Kollegen in den Ländern hat, noch entspricht das Bild der Realität im Alltag.

Ich denke, es könnte ruhig mal etwas öfter gezeigt werden, dass sehr viele schwere Straftaten durch eine Top-Zusammenarbeit der Beamten im Polizeivollzugsdienst, dem LKA und dem BKA gelöst werden. Denn das entspricht der Realität und der täglichen Arbeit von Ihnen und tausenden Polizisten in unserem Land. Und die darf man auch ruhig mal öfter zeigen! Wie wäre es mal mit einem BKA-Kommissar im Tatort, der gute Fälle löst!

Und mehr Realität würde vielleicht auch an anderen Stellen gut tun. Zum Beispiel dort, wo Menschen Teile von Polizeiarbeit – auch die des BKA – wahrnehmen und was das für Auswirkungen auf die Haltung zu Maßnahmen der inneren Sicherheit hat.

Ich meine, unter den Opfern eines Wohnungseinbruchsdiebstahls gibt es sicher eine Mehrheit, die sich darüber ärgert, dass die Polizei die Tat nicht verhindern konnte und eine Minderheit, die eine grundsätzliche Skepsis gegenüber Befugnissen der Polizei hat.

Ich meine, es gibt eine klare Erwartung in der Bevölkerung, dass schwere Straftaten – selbst wenn sie nicht verhindert werden können – zumindest mal aufgeklärt werden und dass eine gefährliche Person, die zur Fahndung ausgeschrieben ist, auch schnell gefasst wird – nicht mit dem Walkie-Talkie, sondern mit moderner IT.

Und ich meine, dass es sehr viele Menschen in unserem Land zutiefst ablehnen, wenn sie sehen, wie in einigen Milieus Polizisten begegnet wird – mit Rudelbildungen, dumpfer Gewalt und unanständigen Beschimpfungen.

Menschen mit viel Geld können sich einen besonders guten Einbruchsschutz leisten – vielleicht sogar einen privaten Wach- oder Sicherheitsdienst. Menschen mit viel Geld können ihre Wohnung oder ihr Haus auch in einen geschlossenen Wohnkomplex verlegen und so Kriminalität einfacher ausweichen als andere. Aber normale Menschen mit einem normalen Verdienst können sich das nicht leisten und es ist die originäre Aufgabe des Staates, dass die Menschen sich das auch nicht leisten müssen.

Jeder, der diese Auffassung teilt, muss dafür sein, dass die Polizei und die Sicherheitsbehörden

- die erforderlichen und gebotenen Mittel und
- die erforderlichen Instrumente bekommen,
- die sie brauchen,
- die sie schützen und
- die ihnen im Einsatz helfen und
- dass Ihnen der gebotene Respekt für Ihre Arbeit gezollt wird – überall in unserem Land.

Mit dem Haushalt 2017 setzen wir jetzt die beispiellose Stärkung der Sicherheitsbehörden des Bundes in Deutschland fort. Das ist die richtige Antwort auf die erheblich wachsende Bedeutung unserer Aufgaben. Das war und ist ein großer Erfolg. Sie sehen deswegen heute einen zufriedenen Bundesinnenminister vor sich.

Aber nicht nur deswegen: Wir haben für die Sicherheit der Bürgerinnen und Bürger in dieser Legislaturperiode unglaublich viel erreicht. Und das setzen wir fort. Ich habe mich in der vergangenen Woche mit meinem Kollegen Maas und führenden Politikern der Koalition auch auf die Umsetzung meines Maßnahmenpaketes geeinigt, das ich im Sommer vorgestellt habe.

Dazu gehört eine

- verbesserte Videoüberwachung an öffentlich zugänglichen Plätzen,
- dazu gehören Bodycams für Polizisten der Bundespolizei,
- dazu gehören Lesesysteme für die Kennzeichen von Kraftfahrzeugen, um Fahnungen schneller und einfacher durchzuführen,
- dazu gehört eine schärfere Bestrafung von gewalttätigen Angriffen auf Polizisten, Justizbedienstete und Rettungskräfte sowie
- eine schärfere Bestrafung von Wohnungseinbrüchen.

Ich bin froh, dass mein Kollege Maas mir zugesagt hat, innerhalb der nächsten Wochen Gesetzentwürfe über solche Strafverschärfungen vorzulegen.

Ich habe meine Rede mit Meldungen begonnen, die ich in Zukunft gerne lesen möchte. Jetzt lese ich Ihnen zum Schluss einige andere vor:

„Schlag gegen international organisierte Rauschgifthändler“.

„Erfolgreicher Abschluss eines EU-Projekts zur Bekämpfung der Eigentumskriminalität durch reisende Täter“.

„Erfolgreiche europaweite Kontrollaktion zur Bekämpfung des Menschenhandels“.

„BKA ermittelt Waffenkäufer im Darknet – mutmaßlich Raubdelikt verhindert“.

„Fünf Millionen Euro Drogengelder gewaschen – Festnahme mutmaßlicher Geldwäscher“.

„Gelungener Schlag gegen international agierende Cyberkriminelle“.

Das sind keine Meldungen aus der Zukunft. Nein, das waren alles – echte – Meldungen des BKA aus den letzten Monaten. Für diese und für alle anderen großen und kleinen Meldungen und für die ganze harte Arbeit, die Sie alle hier jeden Tag für unser Land leisten, danke ich Ihnen.

Sicherheit braucht Menschen, die für Freiheit, Rechtsstaat und Sicherheit eintreten. Das sind Sie. Dafür steht das BKA – heute und ganz sicher auch im Jahr 2020.

Und ich werde meinen Teil dazu beitragen.

* * * * *