Wortprotokoll
der 142. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 7. Juni 2021, 09:30 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Jochen Haug, MdB

Tagesordnung - Öffentliche Anhörung

Antrag der Abgeordneten Benjamin Strasser, Manuel Höferlin, Stephan Thomae, weiterer Abgeordneter und der Fraktion der FDP

Smart Police - Digitalisierung der deutschen Polizei anschieben

BT-Drucksache 19/27172

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Axel Müller [CDU/CSU]
Abg. Susanne Mittag [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Benjamin Strasser [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Irene Mihalic [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Müller, Axel	
SPD	Mittag, Susanne	
AfD	Haug, Jochen Wirth, Dr. Christian	
FDP	Strasser, Benjamin	
DIE LINKE.	Pau, Petra	
BÜNDNIS 90/DIE GRÜNEN	Mihalic, Dr. Irene	
fraktionslos		

Ausschuss für Inneres und Heimat

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 7. Juni 2021, 9.30 Uhr
„Smart Police“

Prof. Dr. Hartmut Aden
Hochschule für Wirtschaft und Recht Berlin

Dr. Simon Egbert
Universität Bielefeld

Holger Gadorosi
Bundeskriminalamt - Leiter des Programms Polizei 2020

Ralf Michelfelder
Präsident des Landeskriminalamts Baden-Württemberg a. D.

Dieter Schneider
Präsident des Landeskriminalamts Baden-Württemberg a. D.

Einziger Tagesordnungspunkt

Antrag der Abgeordneten Benjamin Strasser, Manuel Höferlin, Stephan Thomae, weiterer Abgeordneter und der Fraktion der FDP

Smart Police - Digitalisierung der deutschen Polizei anschieben

BT-Drucksache 19/27172

Stv. Vors. **Jochen Haug** (AfD): Meine sehr verehrten Damen und Herren, ich eröffne die 142. Sitzung des Ausschusses für Inneres und Heimat. Ich begrüße Sie alle sehr herzlich. Mein Name ist Jochen Haug, ich bin der Stellvertretende Vorsitzende des Ausschusses für Inneres und Heimat und werde diese öffentliche Anhörung leiten. Es wird erneut eine öffentliche Anhörung des Ausschusses für Inneres und Heimat sein, die – zumindest in Teilen – als Videokonferenz durchgeführt wird.

Ich danke Ihnen, sehr geehrte Sachverständige, dass sie unserer Einladung auch im Form der Zuschaltung per Videokonferenz nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Ausschuss für Inneres und Heimat und der mitberatenden Ausschüsse zu beantworten. Zunächst begrüße ich den per Video zugeschalteten Sachverständigen Herrn Dr. Simon Egbert. Dann begrüße ich die im Saal anwesenden Sachverständigen: Herrn Professor Hartmut Aden, Herrn Holger Gardorosi, Herrn Ralf Michelfelder, Herrn Dieter Schneider. Begrüßen darf ich auch für die Bundesregierung Herrn Ministerialdirektor Dr. Christian Klos aus dem Bundesministerium des Innern, für Bau und Heimat.

Die Sitzung wird zeitversetzt im Parlamentsfernsehen des Deutschen Bundestages auf Kanal 2 und per Stream auf der Homepage des Deutschen Bundestages übertragen und später über die Mediathek des Deutschen Bundestages für die Öffentlichkeit zum Abruf bereitgestellt.

Schriftliche Stellungnahmen hatten wir erbeten. Für die eingegangenen Stellungnahmen bedanke ich mich bei den Sachverständigen, sie sind an die Mitglieder des Ausschusses für Inneres und Heimat und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über diese Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur Durchführung der öffentlichen Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Von der heutigen Anhörung wird für ein Wortprotokoll eine Abschrift der digitalen Aufzeichnung gefertigt und Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen Details zur Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus Protokoll und schriftlichen Stellungnahmen wird im Übrigen auch ins Internet eingestellt.

Zum zeitlichen Ablauf möchte ich anmerken, dass insgesamt eine Zeit von 9:30 Uhr bis 11:30 Uhr vorgesehen ist. Einleitend möchte ich jedem Sachverständigen die Gelegenheit geben, in einer Erklärung, die fünf Minuten nicht überschreiten sollte, zum Beratungsgegenstand Stellung zu beziehen. Durch die Zuschaltung per Video ist heute unsere Redezeituhr nicht zu sehen, ich bitte daher die Sachverständigen und auch Sie, liebe Kollegen, selbst auf die Einhaltung der Redezeit zu achten.

Nach den Eingangsstatements würden orientiert an Fraktionsrunden mit der Befragung der Sachverständigen durch die Berichterstatterinnen und Berichterstatter sowie weiterer Abgeordneter beginnen. Ich bitte, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die sie die Frage richten wollen. Zu den Frageregeln gilt: In der ersten Fragerunde kann jeder Fragesteller entweder zwei Fragen an einen Sachverständigen, eine gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage richten. Für die zweite Fragerunde würde ich situativ entscheiden, nämlich ob es zeitlich noch möglich ist zwei Fragen an einen Sachverständigen oder eine gleiche Frage an zwei Sachverständige zu stellen oder ob das Zeitfenster es nur noch hergibt, eine

Frage an einen Sachverständigen zu stellen. Wenn Sie damit einverstanden sind, würden wir so verfahren. Danke schön.

Noch einen Hinweis: Die per Video Zugeschalteten möchte ich bitten, ihr Mikrofon so lange ausgeschaltet zu lassen, bis sie ihr Statement halten oder Fragen beantworten, um Rückkopplungen zu vermeiden. Entsprechend alphabetischer Reihenfolge darf ich dann Herrn Professor Dr. Aden um seine Eingangsstellungnahme bitten.

SV **Prof. Dr. Hartmut Aden** (Hochschule für Wirtschaft und Recht, Berlin): Meine Damen und Herren, ich bedanke mich für die Einladung und freue mich, dass Sie sich so kurz vor Ende der Legislaturperiode noch mit diesem wichtigen, auch zukunftsweisenden Thema beschäftigen, das sicherlich auch in Zukunft weiterhin eine große Rolle spielen wird. Ich verweise erst einmal auf meine schriftliche Stellungnahme und bedanke mich bei der Ausschussverwaltung, dass die Stellungnahme kurzfristig verschickt wurde.

Ich möchte zunächst betonen, dass wir hier, anders als das vielleicht in dem Antrag akzentuiert ist, über einen Prozess reden, der nicht erst mit dem anfängt, was man heute als „Digitalisierung“ bezeichnet. Gerade der Polizeibereich war schon Vorreiter in den 1970er Jahren in bestimmten Bereichen dessen, was man heute als Digitalisierung bezeichnen würde, etwa bei der Zusammenschaltung von zentralisierten Datenbanken – damals noch relativ „handgestrickt“. Nichtsdestotrotz haben wir große Diskrepanzen zwischen dem, was sich auf den zentralisierten Ebenen schon seit langem ereignet hat, und dem, was an der Basis ankommt. Da haben wir häufig noch das Problem, dass die Technikausstattung so hinter der Zeit hinterherhinkt, dass die gut ausgebildeten jungen Polizeibeamtinnen und Polizeibeamten im Dienst nicht das nutzen können, was sie in ihrem privaten Leben gewohnt sind. Das sind Diskrepanzen, mit denen man umgehen muss.

Ich denke aber, es ist auch wichtig und von größter Relevanz, in dieser Debatte auch die grundrechtliche Dimension immer wieder in Erinnerung zu rufen und auch in den Vordergrund zu rücken. Das betrifft etwa die Interoperabilität zwischen Datenbanken, wo es eine sehr gute Entwicklung ist, dass auf mehr Datenbestände einfacher zugegriffen werden kann – das kann die Arbeit effizienter und effektiver machen. Gleichzeitig entstehen dadurch aber auch neue Risiken: Wenn etwa ein Datensatz veraltet ist, wenn von vornherein Fehler in diesem Datensatz sind, dann ist durch den größeren Zugriff das Risiko für die Betroffenen größer. Damit muss man, wenn man die Digitalisierung gestaltet, ebenso umgehen, wie mit den Chancen.

Die Chancen liegen aber auch auf ganz anderen Ebenen und da hat uns auch die Datenschutzgrundverordnung (DSGVO) und die für den Polizeibereich geltende JI-Richtlinie, die parallel für den Polizei- und Strafjustizbereich im Jahr 2016 verabschiedet wurde und 2018 in Kraft getreten ist, interessante Ansätze geliefert, die zum Teil in dem Antrag auch vorkommen, zum Teil aber noch nicht. Ich möchte hier insbesondere den Bereich der Transparenz von Polizeiarbeit betonen, der auch in unseren eigenen Forschungen eine wichtige Rolle spielt. Das mag manchen Menschen aus der Praxis zunächst als Widerspruch erscheinen, weil ja Polizeiarbeit häufig sehr stark auf Verschlusssachen, auf die Geheimhaltung von Taktiken und so weiter ausgerichtet ist. Wenn man sich aber näher anschaut, wie diese Problematik gestaltet ist, dann gibt es doch sehr viele Spielräume, gerade gegenüber den Betroffenen von Datenverarbeitung, solche Datenverarbeitungsvorgänge transparenter zu machen.

In einem Forschungsprojekt haben wir etwa in Zusammenarbeit mit der Bundesdruckerei eine Anwendung entwickelt, die es in Zukunft ermöglichen kann, dass Menschen, die von der Polizei kontrolliert worden sind, elektronisch eine Quittung generiert wird – mit sehr wenig Aufwand, also voll digitalisiert. Das gibt auch Menschen, die den Eindruck haben, dass sie vielleicht zu oft von

der Polizei kontrolliert werden, Möglichkeiten, dies zu dokumentieren, liefert aber auch externen Stellen, wie etwa den Polizeibeauftragten, die wir inzwischen in einigen Ländern haben, das entsprechende statistische Datenmaterial. Das ist aus meiner Forschungssicht besonders wichtig vor dem Hintergrund dessen, was man als den procedural justice-Ansatz bezeichnet. Das ist eine Theorie, die in den USA entwickelt worden ist und die zu dem Schluss gekommen ist, dass Polizeiarbeit immer dann auf Akzeptanz stößt, wenn sie von den Betroffenen als fair empfunden wird. Und die Transparenz ist ein ganz zentrales Element dieser Fairness. Ich habe Ihnen in der schriftlichen Stellungnahme etwas näher ausgeführt, wie diese Quittung aussehen könnte und welches technische Verfahren wir dort in Zusammenarbeit mit der Bundesdruckerei entwickelt haben.

Ich möchte hier noch einmal betonen, dass wir im Zusammenhang mit der Digitalisierung der Polizeiarbeit auch sehr stark auf die Missbrauchsrisiken achten müssen. Wir haben das vor einigen Monaten gerade wieder medienwirksam erlebt, als im Zuge des sogenannten NSU 2.0 Daten aus Polizeicomputern abgefragt wurden und wir festgestellt haben, dass das, was uns im Verwaltungsbereich eigentlich selbstverständlich erscheint – nämlich, dass immer nur eine einzige Person auf eine Datenanwendung zugreifen kann und dann im Rahmen der Protokolldaten eindeutig dokumentiert ist, wer den Zugriff hat –, dass das leider in der in der Polizeipraxis nicht überall angekommen ist. Sehr oft ist es tatsächlich noch so, dass in den Dienststellen der Rechner offen ist, mehrere Leute daran arbeiten, weil es praktischer ist oder mal eben einer Pause macht und an den anderen übergibt. Was passiert dann? Dann ist hinterher nicht mehr nachweisbar, wer eigentlich Daten unberechtigt abgefragt hat. Das heißt, da brauchen wir neue und an dem Punkt auch strengere Standards.

Was in dem Antrag aus meiner Sicht auch fehlt, ist die Technikfolgenabschätzung. Das ist ohnehin ein Bereich, der zwar sowohl in der DSGVO als auch in der JI-Richtlinie eindeutig vorgeschrieben ist, aber im Polizeibereich noch nicht richtig angekommen ist. Immer dann, wenn neue Technologien eingeführt werden, muss man vorab eine Bewertung durchführen, damit man nicht erst dann die Risiken wahrnimmt, wenn das Ganze schon fertig ist. Das heißt, das muss sehr frühzeitig in die technischen Konzeptionsprozesse miteingebunden werden. Dafür fehlen meines Erachtens im Polizeibereich bisher die Verfahren, um das auch wirklich frühzeitig sicherzustellen. Ich denke, das ist eine Baustelle, an der im Zuge der Digitalisierung auf jeden Fall weitergearbeitet werden muss.

Das gilt übrigens auch bei „privacy by design“ und „privacy by default“ – das wird ja auch in dem Antrag stark gemacht. Das halte ich auch für einen sehr guten Ansatz, etwa, um damit sicherzustellen, dass die rechtskonforme Nutzung von IT-Systemen im Sicherheitsbereich nicht von den einzelnen Mitarbeiterinnen und Mitarbeitern abhängt, sondern dass die technischen Voreinstellungen bereits so gemacht sind, dass man die Anwendung quasi gar nicht falsch benutzen kann. Da sehe ich noch sehr viel Luft nach oben. Wenn ich mir anschaue, wie diese Vorschriften – das sind verbindliche Vorschriften aus dem EU-Recht, auch aus der JI-Richtlinie – im deutschen Recht umgesetzt worden sind, dann wird meistens nur dieser Begriff wiederholt. Das ist eigentlich nicht mehr als eine Leerformel, und diese Leerformel muss ganz dringend mit Leben gefüllt werden.

Was wir auch in unseren Forschungsprojekten untersuchen, ist die Möglichkeit, die Rechtskonformität der Nutzung von IT-Systemen durch die Bedienerführung sicherzustellen – das halte ich für einen sehr interessanten und sehr wichtigen Ansatz. Wir haben im Bereich der Identitätsfeststellung schon einmal erarbeitet, wie so etwas aussehen kann, und ich denke, wenn ein Gerät, das bei der Polizei im Einsatz ist, von vorn herein so konzipiert ist, dass man es nur rechtskonform nutzen kann, dann wäre tatsächlich für privacy by design und für privacy by default viel gewonnen,

aber der Weg dahin ist noch sehr weit. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir nunmehr zur Stellungnahme von Herrn Dr. Egbert.

SV **Dr. Simon Egbert** (Universität Bielefeld): Vielen Dank für die Einladung und Worterteilung.

Sehr geehrte Damen und Herren, die Digitalisierung bietet selbstverständlich auch für die Polizei erhebliches Potenzial im Hinblick auf die Verbesserung ihrer Arbeit. Allerdings sollte man nicht dem Trugschluss verfallen, zu glauben, dass digitale Technologien gleichsam automatisch eine effektivere und/oder effizientere Polizeiarbeit ermöglichen. Vielmehr ist die erfolgreiche Implementierung von digitalen Technologien nicht nur, aber vor allem bei der Polizei überaus voraussetzungsvoll.

Gleichzeitig ist die Einführung von digitalen Technologien stets mit Risiken verbunden, die konsequent in Rechnung gestellt werden müssen. Diesbezüglich gilt es, zunächst auf ein grundsätzliches Faktum hinzuweisen: Digitalisierte Praktiken sind stets soziotechnische Praktiken. Digitale Technologien sind immer und unumgänglich auch soziale Technologien. Dies impliziert unter anderem, dass algorithmische Analysen keineswegs per se neutrale oder objektive Ergebnisse liefern. Zu glauben, digitale Technologien könnten für neutrale Risikobewertungen sorgen, ist naiv! Bei der Programmierung von Algorithmen und der Auswahl der zu analysierenden Daten sind vielfältige menschliche Entscheidungen zu fällen, die allesamt das Potenzial von Verzerrungen bergen. Die Zusammenarbeit mit Industriepartnern aus der Digitalwirtschaft birgt für die Polizei des Weiteren die Gefahr, mit Instrumenten und Werkzeugen zu arbeiten, die den praktischen Alltag von Polizistinnen und Polizisten nachhaltig prägen, gleichzeitig für diese aufgrund des proprietären Charakters der Algorithmen aber weitestgehend intransparent bleiben. Diese Intransparenz muss so weit wie möglich verhindert werden, da ein kompetenter und kritischer Umgang mit digitalen Technologien sonst nicht möglich ist. Dies gilt ebenfalls für die Bürgerinnen und Bürger, denen gegenüber die Polizei begründungspflichtig ist. Dies gilt selbstredend ebenfalls für Richterinnen und Richter, sowie die Rechtsbeistände von angeklagten Personen, wenn im betreffenden Verfahren solche Arten von Technologien relevant sind. Auch und gerade im Falle digitalisierter Polizeipraktiken muss die Prüfung der Rechtmäßigkeit der erhobenen Vorwürfe umfassend möglich sein.

Fakt ist ferner, dass durch die Digitalisierung der Polizei externe Akteure tief in die operative Arbeit der Polizei eindringen, womit zahlreiche Risiken verbunden sind. Dazu zählt insbesondere, dass sichergestellt werden muss, dass Unbefugte keinen Zugriff auf sensible polizeiliche Daten haben dürfen. Ebenso muss sichergestellt werden, dass so wenige Daten wie möglich aus den Polizeibehörden herausgegeben werden. Zuletzt muss sichergestellt werden, dass auch nach Vertragsende die mit der jeweiligen Software generierten Daten in polizeilicher Hand verbleiben können.

Internationale Studien haben überdies festgestellt, dass digitalisierte Polizeipraktiken zur Folge haben können, Überwachungspotenziale der Polizei zu vergrößern. So schildert die US-amerikanische Soziologin Sarah Brayne in Bezug auf die Nutzung von Palantir-Software des Los Angeles Police Departements das Phänomen der dragnet surveillance – zu Deutsch Schleppnetz-Überwachung –, welches eine substanzielle Ausweitung des überwachenden Blickes der Polizei impliziert: Durch die auf Verbindungsanalysen, sogenannte link analysis, spezialisierte Software der Firma Palantir rücken auch solche Personen in den Fokus, die bis dato noch keinen Kontakt zur Polizei hatten, nur weil sie mit verdächtigen Personen in Kontakt standen. Eine solche Spielart von Kontaktschuld darf keinesfalls Gegenstand polizeilicher Analysetätigkeiten werden.

Und nicht zuletzt bergen anvancierte Datenanalysealgorithmen die Gefahr, einen starken institutionellen Anreiz pro Datensammlung zu erzeugen, da sie umso besser funktionieren, je zahlreicher und heterogener die Daten sind, auf die sie zugreifen können. Entsprechenden Dynamiken muss früh genug Einhalt geboten werden, um weitreichende Rechtsverletzungen zu unterbinden! Herzlichen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zur Stellungnahme von Herrn Gadorosi.

SV **Holger Gadorosi** (Bundeskriminalamt, Wiesbaden): Vielen Dank, meine Damen und Herren, auch ich bedanke mich erst einmal für die Einladung.

Der Antrag zielt meines Erachtens inhaltlich natürlich in die richtige Richtung, aber die Zeit ist ein bisschen darüber hinweggegangen. Wir sind heute mit der Bundesregierung mit den Vorhaben, die gestartet wurden, schon deutlich weiter, als im Antrag zum Teil gefordert wird. Und der Antrag verkürzt natürlich, logischerweise, wie alle Anträge.

Vielleicht ein paar Zahlen zum Hintergrund: Wir haben in der Polizei derzeit in der Republik circa 400 einzelne Systeme, die betrieben werden bei 20 Teilnehmern – macht im Schnitt 20 Systeme pro Teilnehmer. Diese Systeme jetzt alle in einem Hau-Ruck-Verfahren in einem priorisierten Verfahren umzustellen, würde die Kolleginnen und Kollegen, die mit diesen Systemen arbeiten müssen, komplett überfordern. Das braucht Zeit. Die längste Zeit im Wandel brauchen nicht die IT-Systeme, die längste Zeit geht im Wandel für die Kolleginnen und Kollegen drauf, die in neue Systeme eingearbeitet werden müssen.

Die Regierung hat mit dem Programm Polizei 2020 sicherlich ein richtiges Programm aufgesetzt, ein Programm, das eine Harmonisierung und Vereinheitlichung der einzelnen Systeme anstrebt. Und sie ist auf diesem Weg schon große Schritte vorangegangen: Es sind schon Operativsysteme in Betrieb genommen worden, andere Systeme sind noch in der Planung. Es sind Bestandssysteme abgelöst worden, es sind ganz neue Systeme eingeführt worden. Es sind neue fachliche Funktionalitäten eingeführt worden, seien es Analysesysteme, seien es ganz normale Operativsysteme, die jede Polizistin und jeder Polizist für die tagtägliche Arbeit benötigt. Da sind wir auf einem guten Weg und ich glaube, man darf da das Kind nicht mit dem Bade ausschütten. Gut Ding will Weile haben. Man muss einen Schritt nach dem anderen gehen – Evolution statt Revolution. Die polizeiliche Handlungsfähigkeit muss zu jeder Sekunde gewährleistet sein. Es besteht aus meiner Sicht eine große Gefahr der Überforderung, wenn man da zu viel in zu kurzer Zeit möchte. Ich denke, dass der Antrag in die richtige Richtung geht, aber man muss da schrittweise vorgehen, eins nach dem anderen, die richtigen Schwerpunkte setzen. Die polizeiliche Arbeit effizienter gestalten einerseits, gleichzeitig aber auch die fachliche Funktionalität der Systeme optimieren, die Vernetzungen vorantreiben und damit eine noch bessere, optimierte Polizeiarbeit in Deutschland ermöglichen.

Das Ganze natürlich auch international denken. Es ist nicht nur eine rein deutsche Sache. Und bei all dem bitte nicht vergessen: Polizei ist Ländersache – die Bundesregierung hat hier nur beschränkte Möglichkeiten. Wir haben unterschiedliche Polizeiländergesetze, wir haben unterschiedliche datenschutzrechtliche Regelungen. All das muss in Einklang gebracht werden, wenn wir für die deutsche Polizei ein System einsetzten und auch langfristig etablieren wollen. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zur Stellungnahme von Herrn Michelfelder.

SV **Ralf Michelfelder** (Landeskriminalamt Baden-Württemberg): Guten Morgen. Vielen Dank.

Erfolgreiche Polizeiarbeit ist heute wesentlich abhängig von der IT-Ausstattung, aber gleicher-

maßen von der IT-Kompetenz der Polizei. Digitalisierung ist eine wichtige Stellschraube, damit die Polizei mit dem vorhandenen Personal weiterhin ihren Auftrag erfolgreich erfüllen kann, also Gefahren abwehren, Straftaten verhindern, Delikte aufklären. Was Digitalisierung sicherlich nicht macht, ist Geld sparen. Und das muss man immer wieder klarstellen: Digitalisierung spart kein Geld, Digitalisierung kostet Geld. Und zwar erheblich Geld, sowohl in der Erstausstattung als auch in notwendigen Updates von Hard- und Software. Es ist nicht damit getan, das System zu implementieren, sondern man muss das System anschließend auch pflegen. Digitalisierung kann schnellere und bessere Erfolge bringen – mit weniger Personaleinsatz. Dazu gehört, dass die Systeme von den Kolleginnen und Kollegen vor Ort akzeptiert werden. Die Arbeit muss vor Ort beginnen, nicht irgendwo in irgendwelchen Rechenzentren, sondern die Akzeptanz muss vor Ort da sein. Und die entsteht am besten dadurch, dass die Kolleginnen und Kollegen vor Ort Erfolge erzielen. Denen ist im Zweifelsfall egal, ob es irgendwo in der Republik ein Datawarehouse oder einen anderen schönen Anglizismus gibt, wenn bei ihnen die Informationen nicht oder nur tröpfchenweise eintrudeln.

Ich habe da ein paar Beispiele: Wenn ein bundesweiter Großeinsatz mit Unterstützungskräften aus nahezu allen Bundesländer über einen Messenger geführt wird und man dann feststellt, dass die Messenger der einzelnen Bundesländer nicht miteinander kompatibel sind und der Einsatz dann über Threema geführt wird, dann ist das einfach nicht mehr zeitgemäß. Zumal für die Kolleginnen und Kollegen aus Baden-Württemberg Threema gar nicht auf dem dienstlichen Handy installiert werden kann. Die mussten dann auf ihre privaten Handys zurückgreifen und dort die Führungssoftware Threema installieren.

Wenn eine Frau zum Polizeirevier kommt, eine Anzeige erstattet über eine Nötigung mit Bedrohungssachverhalt über E-Mails, die sie auf ihrem Smartphone bekommt – und 98 Prozent der Bevölkerung haben heutzutage ein Smartphone, viele haben gar nichts anderes mehr. Smartphone ist nicht nur ein Telefon, es ist das Office, es ist die Kamera, es ist im Grunde sowohl der geschäftliche als auch der Liebesbrief-Postkasten und was auch immer mehr. Wenn die Frau mit dem Handy auf das Revier kommt und sagt: „ich kann das nicht ausdrucken“ und der Kollege kann es auch nicht und man dann in der Not das Handy auf den Fotokopierer legt, um so den Text vom Handy ab zu fotokopieren, dann ist das nicht Digitalisierung in dem Sinne, wie es die Kollegenschaft erwartet.

Andererseits gibt es aber auch ein Riesenpotenzial: Tödlicher Verkehrsunfall in Stuttgart, bei dem ein Raser mit seinem Sportwagen auf einen Kleinwagen eines jungen Paares gefahren ist. Das junge Paar, da sind beide ums Leben gekommen. Am nächsten Tag stand in der Zeitung, dass der Sachverständige davon ausgeht, dass der Sportwagenfahrer mit mindestens 80 km/h gefahren sein soll. Das hat das Landeskriminalamt Baden-Württemberg zum Anlass genommen, sich selbst um diesen Fall zu kümmern, die Steuergeräte auszubauen, um dann feststellen zu müssen, dass der Sportwagenfahrer vier Sekunden vor dem Aufprall noch mit 160 km/h und nicht bloß mit 80 km/h durch die Stadt gefahren ist und beim Aufprall immerhin noch 140 km/h Geschwindigkeit hatte. Die Staatsanwaltschaft hat daraufhin die Anklage auf Mord erweitert. Dazu muss man es aber wissen, um es nutzen zu können.

Digitale Tatorte sind heutzutage der Standard, nicht mehr die Ausnahme. An jedem Tatort, wo wir noch haptische, analoge Spuren haben, haben wir auch digitale Spuren. Wir haben sogar Tatorte, an denen wir nur noch digitale Spuren haben. Das ist auch mit riesigen Datenmengen verbunden: Im Megabyte-Bereich sind wir schon längst nicht mehr, Gigabyte wird abgelöst von Terabytes an Datenmengen. Das LKA Baden-Württemberg hat in einem Ermittlungsverfahren 1,2 Petabytes an Daten sichergestellt. Ein Petabyte ausgedruckt an Text auf

DIN A 4-Blätter bedeutet einen Stapel von 50.000 km Höhe! Händisch durchsehen geht da nicht mehr.

Wie können wir die Digitalisierung in der Polizei optimieren? Aus meiner Sicht gibt es fünf wesentliche Stellschrauben:

Erstens: Polizeibeamte in der Ausbildung für die Digitalisierung befähigen. Die müssen verstehen, was für Potenziale die polizeilichen Tools bieten und gleichzeitig müssen sie die Sensibilität haben, digitale Spuren überhaupt zu erkennen – also so eine Art digitaler Führerschein. Es macht keinen Sinn, einem ein großes Auto hinzustellen und der hat keinen Führerschein, um damit zu fahren.

Zweitens braucht es die technische Infrastruktur. Zentrale Systeme sind gut, aber nur dann, wenn sie auch überall performant genutzt werden können. Und es braucht natürlich medienfreie Ermittlungsarbeit, beispielsweise durch Tablets im Streifenwagen. Wenn ich den Einsatz auf mein Tablet bekomme, und kann draußen vor Ort über das Tablet gleich zurückschreiben, dann spart man die anschließende Schreibarbeit auf dem Revier, die ich dann dafür nutzen kann, mehr präsent zu sein auf der Straße.

Drittens muss die Analysefähigkeiten der forensischen Labore ausgeweitet werden. Angesichts dieser Datenmassen braucht es auch leistungsstarke Systeme, Analyse-/Auswertesysteme, in den Zentralstellen der Polizei und skalierbare Speicher.

Wir brauchen eine größere Auswertekompetenz bei der Polizei – der Allround-Ermittler, der montags Vernehmungen durchführt und dienstags diese Datenmassen auswertet, das funktioniert heute nicht mehr. Das FBI hat schon längst umgestellt und hat neben den Ermittlern, also neben den Agents auch Intelligent Analysts, also reine Datenermittler, im Einsatz, die parallel zu den Ermittlern die Tools kompetent nutzen. Ich nutze Word wie eine elektrische Schreibmaschine und Excel wie ein Tabellenrechnungsprogramm, weil ich die ganzen hilfreichen Tools, die dahinter stecken, gar nicht kenne. Wenn wir teure Software kaufen und sie dann nur oberflächlich nutzen, ist das schade und der Nutzen ziemlich begrenzt.

Abschließend: Wir müssen die Beschaffungsprozesse beschleunigen. Der Bürger ist gewohnt, dass er, wenn er ein Problem hat, 110 anruft und die Polizei erscheint. Die Polizei hat ein Problem, das man IT-technisch lösen kann und es dauert fünf Jahre!? Nicht von dem Zeitpunkt an, in dem man das Problem hat, sondern von dem Zeitpunkt an, an dem man vereinbart hat, es zu lösen. Wenn Vergabeverfahren über zwei Jahre dauern, wenn wir dann aber auch darüber hinaus selbstkritisch nicht in der Lage sind, ein Produkt von der Stange zu kaufen, sondern meinen, wir brauchen immer einen Maßanzug, dann schwindet erstens dadurch die Akzeptanz und zweitens entstehen dann Parallelbeschaffungen, die wir ausgehend von der Saarbrücker Agenda gar nicht mehr wollen. Danke schön.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zur Stellungnahme von Herrn Schneider.

SV **Dieter Schneider** (Landeskriminalamt Baden-Württemberg): Vielen Dank, meine sehr verehrten Damen und Herrn.

Digitalisierung in der Polizei ist ein facettenreiches und sehr breites Thema mit ganz unterschiedlichen Dimensionen. Es geht um die Ausstattung mit digitalen Arbeitsmitteln, es geht um digitale Kommunikation, es geht um digitale Aktenführung, digitale Forensik, die gerade angeklungen ist, und vor allem auch um digitales Know-how bei den Beschäftigten für die Nutzbarmachung im eigenen Aufgabenbereich, aber auch für das Erkennen der allgegenwärtigen digitalen Ansatzpunkte, um nicht zu sagen Spuren. Ich möchte den Schwerpunkt des Eingangsstatements auf das Thema der Digitalisierung des Informationswesens, das Informationsmanagement, legen. Dazu fünf Kernaussagen:

Erstens: Innere Sicherheit gewährleisten, Gefahren

abwehren und Kriminalität bekämpfen setzen voraus, dass alle verfügbaren und relevanten Informationen in einem Gesamtsystem für die Polizei von Bund und Ländern nutzbar sind. Das ist eine Kernaussage der Saarbrücker Agenda, der uneingeschränkt zuzustimmen ist: Informationen sind das Kapital der Polizei schlechthin, Informationen über Straftäter, über Straftaten, über Phänomene, über Entwicklungen, über Gefahrenlagen, über sicherheitsrelevante Umfeldfaktoren – das sind entscheidende Grundlagen für gute und erfolgreiche Polizeiarbeit. Eine Beurteilung der Lage im operativen Einzelfall oder im Großeinsatz hängt entscheidend davon ab, wie umfassend und fundiert Informationen sind. Und je umfassender die Lagebeurteilung, umso zielgerichteter sind polizeiliche Maßnahmen. Verfügbarkeit der Informationen – das ist das strategische Ziel der Saarbrücker Agenda.

Der zweite Punkt: Digitalisierung darf kein Selbstzweck sein. Mit digitalen Methoden werden Strukturen und Prozesse in Organisationen nicht automatisch besser. Werden schlechte Prozesse einfach nur digitalisiert, sind es anschließend schlechte digitale Prozesse. Also sind – allen Bemühungen um Digitalisierung vorgeschaltet – Situationen und Prozesse zu analysieren, Potenziale zu erkennen und dann optimierte Strukturen und Prozesse zu digitalisieren. Ich empfehle Vorsicht vor Schnellschüssen und dem scheinbaren Wundermittel der Digitalisierung. Digitalisierung darf nicht reduziert werden auf ein IT-Vorhaben, sondern ist Teil, aber auch Anstoß einer Organisationsentwicklung. Wenn allerdings die Organisationshoheit bei 20 Teilnehmern liegt, wie beim Programm 2020, mag man erahnen, wie langwierig sich die Verständigung auf einen gemeinsamen Nenner als Voraussetzung einer Digitalisierung gestalten kann.

Dritter Punkt: Die Umsetzung der Saarbrücker Agenda ist fachlich hoch anspruchsvoll und im föderalen Kontext extrem komplex. Die Herausforderungen für die Kriminalitätsbekämpfung und Abwehr von Gefahren haben in den letzten Jahren permanent und mit zunehmender Geschwindigkeit zugenommen – ich denke, das ist jedem bewusst. Die Sicherheitsorgane haben mit vielfältigen, angepassten Konzepten spezifisch reagiert. Kernelement der polizeilichen Konzepte zur Gewährleistung von Sicherheit und Ordnung ist das Informationsmanagement und so sind aus dieser Entwicklung heraus unzählige Meldedienste klassischer Art, Falldateien, Auswerteprojekte, Analyseeinrichtungen entstanden – jedes für sich einleuchtend. In der Summe ist daraus allerdings ein Flickenteppich entstanden. Informationen werden phänomenspezifisch in Datensilos gespeichert und nicht übergreifend zusammengeführt. Datenverarbeitungssysteme, z. B. die Vorgangsverarbeitung als das umfassendste in der Anbindung befindliche System, reichen in ihrem Entwicklungsstand von topmodern bis zum DV-technischen Steinzeitalter. Und in diese Situation kommt die Ansage der Saarbrücker Agenda: Harmonisieren und Konsolidieren! Und dann folgt die Reaktion: Keiner möchte von seinen gewohnten Standards abweichen und hat dafür zumeist auch gute Gründe. Fakt ist: Polizeiarbeit in deutschen Ländern und Landen ist nicht gleich Polizeiarbeit. Das Informationsmanagement als Kernelement zu harmonisieren, ist, das ergibt sich aus diesem Blitzlicht, extrem aufwendig und erfordert langwierige Abstimmungen. Und dabei darf kein Teilnehmer abgehängt werden, sonst haben wir Informationslücken – ein zweites Problemfeld bei der Umsetzung. Die Operation Harmonisierung muss am lebenden Organismus erfolgen. Ein Shutdown, ein Ausstieg und sei er auch nur kurz – Herr Gadorosi hat von einer Sekunde gesprochen – aus unserem Informationsverbund, ist sicherheitstechnisch nicht zu verantworten. Eine Planung auf der grünen Wiese wäre sicher sehr viel einfacher, als die Umwandlung dieser heterogenen Landschaft in einen konsolidierten Informationsverbund.

Vierter Punkt: Stärkung des Datenschutzes - ja, aber nicht auf Kosten der Sicherheit. Stärkung des

Datenschutzes durch Technik ist eines der strategischen Ziele der Saarbrücker Agenda und des Programmes 2020 – unbestritten, richtig und gut so. Es wird in den Konzepten zur Umsetzung in vielfältiger Weise berücksichtigt mit redundanzfreier Datenhaltung, Kennzeichnung der Daten mit dem Zweck der Erhebung, Zugriffe nur nach einem Rechte- und Rollenkonzept, individualisiert, spezifisch, Nutzung nur bei Zweckänderung oder bei vergleichbarer Eingriffsintensität und so weiter, Sie kennen das. Der entscheidende fachliche Mehrwert des künftigen Informationsmanagements muss aber darin liegen, dass die Verbundrelevanz der Daten der Teilnehmer durch das System geprüft und angezeigt wird. Das ist ein Paradigmenwechsel. Der schwarze Golf in München bei einem Einbruch – diese Information muss zusammengeführt werden können mit der Unterschlagung an der Tankstelle in Dresden und dem Ausspähversuch einer Villa in Berlin. Nach heutigem Stand haben wir bei diesem Beispiel drei Informationen aus drei Teilnehmern, die nicht zusammengeführt werden. Nach dem Paradigmenwechsel muss künftig die Information verfügbar geteilt werden, um sie automatisiert zusammenzuführen und dann allen Bedarfsträgern zur Verfügung zu stellen. Dieser Paradigmenwechsel ist fachlich notwendig und er muss auch datenschutzrechtlich vollzogen werden.

Letzter Punkt: Das Programm Polizei 2020 kann zu einem Erfolgsmodell werden, trotz der großen hier nur skizzierten Schwierigkeiten. Die Umsetzungsgeschwindigkeit mit Zwischenzielen muss erhöht werden! Nach mehr als vier Jahren seit Verabschiedung der Saarbrücker Agenda fragt man vielerorts nach der Realisierung von konkreten operativen Projekten für die polizeiliche Praxis. Die Saarbrücker Agenda vom 30.11.2016 selbst, Sie wissen das, war nach jahrelangen Diskussionen im Bund-Länder-Kontext ein Durchbruch für das Bestreben nach Konsolidierung und Harmonisierung des Informationsmanagements. Mit der Vereinbarung des Polizei-IT-Fonds konnte in vergleichbar schneller Zeit die finanzielle Basis für ein gemeinsames Vorgehen geschaffen werden. Die Teilnehmer bringen sich zudem personell in erheblichem Umfang in die Umsetzung ein und übernehmen notwendigerweise Verantwortung in Themenführerschaften. Damit haben wir organisatorisch für das Programm einen richtigen Verbund. Auf die Schwierigkeiten habe ich hingewiesen: In der Anfangsphase der Programmumsetzung war die Grundlagenarbeit für die Erarbeitung von Möglichkeiten, diese Ziele umzusetzen, herausragend, aber mangels vergleichbarer Vorhaben auch sehr aufwendig. Heute haben wir Projekte und Programmelemente – in der Zahl mehr als 30 – an denen bereits konkret gearbeitet wird. Das Programm ist damit auf einem guten Weg. Danke schön.

Stv. Vors. **Jochen Haug** (AfD): Danke schön für die Stellungnahmen. Dann kommen wir jetzt zur ersten Fragerunde. Wir beginnen bei der CDU/CSU-Fraktion und Herrn Müller.

BE Abg. **Axel Müller** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Vielen Dank auch für die Stellungnahmen der Sachverständigen. Ich habe zwei Fragen an Herrn Schneider. Die erste Frage zielt darauf ab, dass das digitale Leitbild für die Polizei, wie es der Antrag vorsieht, auch eine Bewertung der Forderungen vor dem Hintergrund der Bestrebungen des Programms Polizei 2020 mit sich bringt. Sie haben einen Teil schon gesagt in der Kürze der Ihnen zur Verfügung stehenden Zeit. Ich würde Sie aber bitten, vielleicht noch einmal etwas ausführlicher zu schildern, wie wir mit diesem Programm „Polizei 2020“ im Grunde schon jetzt den Forderungen des Antrags – so meine Sicht der Dinge – entsprechen.

Die zweite Frage geht in eine ähnliche Richtung: Es gibt ja im Antrag den Vorschlag eines Digitalpaktes. Das unterstellt meines Erachtens, dass – so bewertet das aus meiner Sicht der Antrag – in diesem Programm Polizei 2020 nur Dinge umgesetzt werden, die schon beschlossen sind, also dass im Grunde ein Aufgabenkatalog abgearbeitet wird, der nicht einer gewissen Dynamik unterliegt und

auch keine Erweiterungen beinhaltet. Da würde mich interessieren, ob das so ist oder ob auch weitere Dinge dazugekommen sind oder auch dazukommen werden, die dann da im Laufe des Prozesses zusätzlich abgearbeitet werden. Danke schön.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zur AfD-Fraktion und Herrn Dr. Wirth.

Abg. **Dr. Christian Wirth** (AfD): Vielen Dank, Herr Vorsitzender, vielen Dank an die Berichterstatter.

Meine erste geht auch an Herrn Schneider: Sie kommen ja aus Baden-Württemberg und eine konkrete Frage dazu: Wir wurden ja letztes Jahr während des Lockdown aus Baden-Württemberg mit dem neuen Gruppenbild „Partyszene“ bedacht. Müssten Ihrer Ansicht nach nicht durch die Bundespolizei und die Polizeien der Länder in der polizeilichen Eingangsstatistik der Aufenthaltsstatus von Tatverdächtigen miterfasst werden, wenn es um bestimmte Kriminalität und Analyse geht, wegen Tatörtlichkeiten, zum Beispiel Bahnhöfen und öffentlichen Plätzen, gegebenenfalls vielleicht sogar doppelte Staatsbürgerschaften, da ja offensichtlich ist, dass gewisse Personen die öffentliche Gewalt nicht unbedingt respektieren.

Meine zweite Frage geht an Professor Aden: Wie weit darf aus Ihrer Sicht der Einsatz von künstlicher Intelligenz bei der Kriminalitätsbekämpfung gehen – Stichwort: Gesichtserkennung an öffentlichen Bahnhöfen und Plätzen, aber auch im Hinblick auf die Analyse von Datenbanken?

Eine fundierte Analyse von Kriminalstatistiken braucht nach unserer Ansicht auch Tatorte, Aufenthaltsstatus und ähnliches, die man gegebenenfalls im Ausländerzentralregister abfragen muss. Dazu meine Frage. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zur SPD-Fraktion und Frau Mittag.

BEin Abg. **Susanne Mittag** (SPD): Ja, danke. Ich habe zwei Fragen an Herrn Gadorosi und zwar – eines ist ja schon eingeführt worden, 2016 hatte man erwartet, dass im Jahr 2020 Polizei 2020 fertig wäre, aber da haben sich offensichtlich noch einige Widrigkeiten ergeben – dazu hätte ich dann die nächsten Fragen, weil das ist ja nicht nur Digitalisierung, sondern das ist auch ein Systemwechsel, das ist schon erwähnt worden, und zwar im laufenden Betrieb. Welche Widrigkeiten haben sich denn im Rahmen dieser Umsetzung ergeben, z.B. Probleme, die vorher nicht absehbar waren, das ist ja ein riesen Gebiet? Und wie weit sind Sie mit der Umsetzung, wann ist geplant, die abzuschließen, in welchem Rahmen ist geplant, die dann auch weiterzuführen? Das ist ja immer ein laufender Prozess.

Die zweite Frage wäre: Das ist die Hardware-Variante, wir haben aber auch noch eine menschliche Variante davor. In dem Antrag ist unter anderem dargelegt worden, Homeoffice für alle, das ist natürlich nicht möglich.

BE Abg. **Benjamin Strasser** (FDP): Das stimmt ja gar nicht!

BEin Abg. **Susanne Mittag** (SPD): In welchem Rahmen gibt es denn Möglichkeiten der Büronutzung, beim Tatort zum Beispiel, in Fahrzeugen? Also gerade bei der Polizei ist das ja eine riesige Bandbreite, wo angewandt werden muss, damit es auch schnell geht, unter Stress geht, unter Zeitdruck – wie weit sind wir denn mit der Umstellung der Menschen vor Ort? Wir haben ja nicht nur Polizisten in der Ausbildung, sondern es stehen auch welche kurz vor der Pensionierung, auch altersmäßig im Mittelbau – wie weit ist man da?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir nunmehr zur FDP-Fraktion und Herrn Strasser.

BE Abg. **Benjamin Strasser** (FDP): Vielen Dank. Zunächst einmal möchte ich sagen, dass Polizei 2020 sicher ein erster, wichtiger Schritt ist. Nur darf man auch nicht dem Trugschluss unterliegen,

dass das die Digitalisierung der Polizei ist. Es ist ein Aspekt der Digitalisierung der Polizei, weil der Kern ist ja die Schaffung eines gemeinsamen Datenhauses von Bund und Ländern. Das ist Polizei 2020. Aber wenn man einmal in die Bundespolizei und das Bundeskriminalamt schaut, was allein die technische Ausstattung angeht, dann sind wir da schon relativ nah an dem, was Herr Michelfelder aus der baden-württembergischen Polizei geschildert hat und deswegen habe ich auch zwei Fragen an Herrn Michelfelder. Die erste Frage ist: Herr Michelfelder, Sie hatten sich in der Vergangenheit immer wieder sehr energisch für das Thema künstliche Intelligenz auch zur Nutzung in Polizeibehörden eingesetzt. Sie hatten vorhin auch angedeutet mit den Aktenordnern, wenn man die händisch auswerten würde, dass es nach menschlichem Ermessen gar nicht möglich sei. Da wäre meine Frage, was Sie hier als unabdingbar auch an technischen Voraussetzungen sehen. Und ob das von dem Programm Polizei 2020 abgedeckt ist?

Und meine zweite Frage: Sie hatten das so schön als digitalen Führerschein bezeichnet – wie schaffen wir die Kompetenzen innerhalb der Polizeibehörden, um die Software überhaupt anzuwenden. Wir schlagen ja in unserem Antrag sowohl die Gründung einer gemeinsamen Digital-Akademie von Bund, Ländern und Kommunen vor, als auch eigene Ausbildungszüge zu schaffen, was IT-Fachkräfte angeht, die diese Infrastruktur bei der Polizei auch entsprechend pflegen. Was würden Sie denn darüber hinaus noch als erforderlich sehen, um diese digitalen Kompetenzen zu stärken, damit es in der Praxis auch wirklich gelebt wird. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zur Fraktion DIE LINKE. und Frau Pau.

BEin Abg. **Petra Pau** (DIE LINKE.): Danke schön an alle Sachverständigen.

Meine Fragen richten sich an Herrn Egbert: Allgemein wird ja erklärt, dass algorithmenbasierte Datenanalyse tatsächlich nicht vorurteilsbasiert ist, anders als menschliche Analysen. Wir haben uns in der Vergangenheit ja sehr viel, zum Beispiel im NSU-Untersuchungsausschuss, damit beschäftigt, wie Vorurteile Ermittlungen beeinflussen. Wie sehen Sie das? Teilen Sie den Optimismus, dass algorithmenbasierte Datenanalysen einen Beitrag zu einer diskriminierungsfreien Polizeiarbeit sein können oder spricht auch etwas dagegen?

Und die zweite Frage: Sie haben schon in Ihrer Stellungnahme darauf hingewiesen, dass die Polizei, derzeit zumindest, darauf angewiesen ist, Produkte für Datenhaltung und -analyse bei Privatunternehmen einzukaufen. Wie kann aus Ihrer Sicht verhindert werden, dass hier eine Blackbox entsteht und welche Sicherungen müssten aus Ihrer Sicht tatsächlich eingebaut werden, dass diese Daten weder während des Einsatzes dieser Produkte noch nach Auslaufen der dazugehörigen Verträge die Polizei verlassen?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen nunmehr zur Fraktion BÜNDNIS 90/DIE GRÜNEN und Frau Dr. Mihalic.

BEin Abg. **Dr. Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Auch von mir erst einmal herzlichen Dank an die Sachverständigen.

Ich habe zwei Fragen an Professor Aden. Und zwar ist es ja so, dass die FDP in ihrem Antrag fordert – das ist eben auch schon ein paarmal genannt worden – dass im Polizeibereich auf Basis künstlicher Intelligenz oder maschinellem Lernen Routinetätigkeiten automatisiert oder auch Dinge analysiert werden. Da würde mich Ihre Bewertung aus verfassungsrechtlicher Sicht einmal interessieren – vor allen Dingen, wenn wir darüber nachdenken, dass es ja vielleicht nicht nur um die Auswertung bestimmter Datenbestände geht, sondern vielleicht auch mit Blick auf predictive policing – also man kann ja mit künstlicher Intelligenz und solchen automatisierten Analysen noch vielerlei Dinge anstellen und da würde mich Ihre Bewertung interessieren. Wie weit kann man

da gehen, beziehungsweise wo sind eben auch Grenzen gesetzt, wenn man zum Beispiel an predictive policing denkt?

Über das Projekt Polizei 2020 ist jetzt auch schon viel gesprochen worden. Deswegen kann ich mir da einleitende Worte sparen. Aber auch da würde mich Ihre Einschätzung, Herr Professor Aden, zum Datenhaus beim BKA interessieren. Gegenüber diesem geplanten Datenhaus bestehen einfach insgesamt erhebliche datenschutzrechtliche und auch verfassungsrechtliche Bedenken. Und so hat nicht zuletzt der BfDI ja wiederholt darauf hingewiesen, dass umfassende Informationen auch über Personen zur Verfügung gestellt werden, die hierzu gar keinen Anlass geben, zum Beispiel Zeugen oder auch Geschädigte und deswegen würde mich da Ihre Einschätzung noch interessieren, wie Sie das verfassungsrechtlich betrachten.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann haben wir die Fragen abgeschlossen, kommen zur Antwortrunde und starten wieder in alphabetischer Reihenfolge bei Herrn Professor Aden.

SV **Prof. Dr. Hartmut Aden** (Hochschule für Wirtschaft und Recht, Berlin): Vielen Dank für die interessanten Fragen.

Ich fange mit denen an, die sich auf die künstliche Intelligenz beziehen, sowohl die Frage von Herrn Dr. Wirth, als auch die von Frau Dr. Mihalic. Nach meiner Einschätzung müssen und können wir damit rechnen, dass auch im Polizeibereich die Nutzung selbstlernender Systeme in Zukunft eine größere Rolle spielen wird als in der Vergangenheit. Da befinden wir uns erst ganz am Anfang der Entwicklung, da ist eine sehr große Dynamik dahinter. Aber wir wissen auch, wo die Risiken liegen. Und diese Risiken müssen auch hier von vornherein berücksichtigt werden. Ich hatte ja schon eingangs die Datenschutzfolgenabschätzung genannt, und das gilt natürlich für solche Technologien, die eine sehr starke Eigendynamik entwickeln können, umso mehr. Da haben wir Risiken, die –wenn man sich etwa Science Fiction-Filme anschaut – so weit gehen können, dass am Ende der Mensch die Entscheidungsmacht verliert. Es gibt ja auch in dieser Legislaturperiode eine Enquetekommission hier im Bundestag, die Europäische Kommission hat sich dazu geäußert, es gibt jetzt auch einen Gesetzgebungsvorschlag auf europäischer Ebene zur künstlichen Intelligenz. Das heißt, es ist überall deutlich geworden, dass dort regulatorischer Handlungsbedarf besteht. Man sollte die künstliche Intelligenz nicht verdammen, aber dafür sorgen, dass sie verantwortungsvoll genutzt wird, und da gehören bestimmte Regeln dazu.

Ich hatte eingangs auch schon die Transparenz erwähnt – das gilt für die künstliche Intelligenz im besonderen Maße. Eine wesentliche Anforderung an KI-Lösungen ist, dass die Entscheidungen am Ende noch nachvollziehbar sind. Auch dort, wo das System selbst gelernt hat, also sich gegenüber der ursprünglichen Programmierung weiterentwickelt hat. Man braucht dann außerdem ein menschliches Letztentscheidungsrecht. Das heißt, man darf sich nicht auf die Maschine verlassen und auch nicht auf die Ergebnisse dessen, was dort herausgekommen ist, so fixieren, dass gar keine andere Entscheidung mehr möglich ist. Bei diesem Punkt sehe ich übrigens die größten Risiken, weil wir in der Vergangenheit immer wieder gemerkt haben, dass auch im Sicherheitsbereich Menschen durchaus technikgläubig werden können. Sie erinnern sich vielleicht alle noch an den Fall, als DNA an Wattestäbchen klebte, in dem man sich erst später darüber gewundert hat, dass diese DNA von jemandem stammte, der die Wattestäbchen in der Fabrik verpackt hatte und nicht etwa von 25 verschiedenen Tatorten. Gerade da sehe ich bei der KI erhebliche Risiken, dass diejenigen, die damit arbeiten, diese Systeme irgendwann so spannend und überzeugend finden, dass sie nicht mehr genügend nachdenken, ob eigentlich die erzielten Ergebnisse überhaupt vernünftig sind. Und da sehe ich die ganz große Baustelle – übrigens auch für die Gesetzgebung –, da von vorn herein einen Riegel vorzuschieben, dass solche KI-Lösungen sich nicht

so verselbstständigen, dass am Ende völlig unsinnige, aber auch viel zu grundrechtseingriffsintensive Konsequenzen damit verbunden sind.

Es gibt aber auch interessante Chancen und wir müssen natürlich sehen, dass etwa im Bereich der Kriminalität auch die Manipulation durch künstliche Intelligenz intensiv genutzt wird. Wir haben gerade ein neues Forschungsprojekt angefangen, in dem wir uns mit deep fakes beschäftigen. Ein großes Problem besteht darin, dass man heute im Internet viele Bilder, aber auch Videos findet, die mithilfe von künstlicher Intelligenz so professionell gefälscht sind, dass die Fälschung für die normalen Nutzerinnen und Nutzer schwer zu erkennen ist. Das sind einerseits Betrugsszenarien, aber wenn man sich etwa die US-Wahlkämpfe anschaut, dann geht das weit in den politischen Prozess hinein, wo auch Manipulationsmöglichkeiten bis hin zur öffentlichen Meinung bestehen. Da sehe ich ganz großen Handlungsbedarf. In diesem Projekt mit dem Titel „FAKE-ID“ wollen wir versuchen, mithilfe künstlicher Intelligenz Wahrscheinlichkeiten zu detektieren, ob ein Video-Stream echt oder gefälscht ist. Auch da haben wir eine ganze Reihe von Landeskriminalämtern mit im Boot, sodass wir uns auch da für die Praxis interessante Ansätze erhoffen.

Um auch noch einmal auf die Frage von Frau Dr. Mihalic stärker einzugehen: Die KI hat selbstverständlich auch ein paar verfassungsrechtliche Grenzen und das sind die ganz normalen strafjustiziellen Grundrechte wie etwa die Unschuldsvermutung. Das heißt also, der Tatverdacht darf nicht durch die KI allein generiert werden, sondern da müssen immer noch einmal Menschen draufschauen. Vielleicht müssen sogar in Zukunft mehr Menschen draufschauen, als das in der Vergangenheit der Fall war. Das war ja auch eine Schlussfolgerung der NSU-Untersuchungsausschüsse: Dass es eben manchmal nötig ist, dass jemand auch noch einmal from a distance auf einen Ermittlungskomplex schaut, ob das Ganze überhaupt plausibel ist, was die Maschine dort ausgerechnet hat. Da sehe ich ganz neue Herausforderungen und ich denke auch, da müsste tatsächlich die Gesetzgebung frühzeitig tätig werden, damit man nicht erst dann, wenn die ersten großen Skandale passiert sind, merkt, dass man irgendetwas falsch gemacht hat.

Und dann haben wir bei den Datenpools – das war ja die zweite Frage von Frau Dr. Mihalic –die Problematik der Zweckbindung. Das ist ein Grundsatz, der aus meiner Sicht durchaus auch weiterhin aktuell ist. Das heißt, Daten, die staatliche Behörden erheben, sind erst einmal für einen bestimmten Zweck erhoben worden und die sollten auch weiterhin erst einmal nur für diesen Zweck verwendet werden können. Das ist eine Problematik, die sehr viel diskutiert worden ist in den letzten Jahren, auch aufgrund der Rechtsprechung des Bundesverfassungsgerichts. Darauf will ich jetzt nicht im Einzelnen eingehen. Ich denke aber, man sollte die Zweckbindung im Zuge der Schaffung von Datenpools nicht vollkommen aufgeben. Sie hören schon: Ich bin nicht prinzipiell dagegen, die Daten stärker miteinander zu verknüpfen, um auch gerade solche übergreifenden Ermittlungskomplexe naheliegender fortführen zu können. Aber auch da brauchen wir sehr viel intensivere Verfahrensvorkehrungen, damit am Ende tatsächlich klar ist: Welcher Zweck ist das jetzt genau gewesen. Da wird man also sehr viel mehr in die Strukturen investieren müssen als das im Moment in den Gesetzen vorgesehen ist. Und ich meine auch, da müsste in den Gesetzen selbst schon sehr viel mehr vorgegeben werden, als das heute der Fall ist.

Um dann noch den zweiten Teil der Frage von Herrn Dr. Wirth zu beantworten: Auf welche Datenbanken konkret zugegriffen werden kann, ist wiederum eine Frage der Berechtigungskonzepte. Auch da bin ich der Meinung, dass die Gesetzgebung hier sehr viel klarere Vorgaben machen sollte, sodass es nicht ausreicht, wie es bisher häufig in den Gesetzen steht, nämlich dass die Erforderlichkeit für die Aufgabenerfüllung ausreicht. Da

werden wir sicherlich zu gesetzgeberischen Lösungen kommen müssen, bei denen die Aufgaben sehr viel klarer definiert sind, damit von der Zweckbindung noch genügend übrig bleibt. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen nunmehr zu Herrn Dr. Egbert.

SV **Dr. Simon Egbert** (Universität Bielefeld): Vielen Dank. Vielen Dank für die Fragen.

Stichwort Algorithmen, Diskriminierung: Selbstverständlich kann ein Algorithmus nicht per se und gleichsam automatisch dafür sorgen, dass Entscheidungen oder Analyse-Tätigkeiten der Polizei diskriminierungsfreier werden. Ich habe in meiner schriftlichen Stellungnahme ja auch das „Garbage in – Garbage out-Modell“ noch einmal bildlich eingefügt. Das zeigt, wie ich finde, relativ schön, dass, wenn man einen schlechten Algorithmus – sprich ein schlechtes Modell – hat, dass dann das Endresultat, auch wenn die Input-Daten korrekt und diskriminierungsfrei sein sollten – wenn der Algorithmus das nicht ist, dann hat man am Ende auch ein diskriminierungsbezogenes Ergebnis. Das gilt gleichermaßen, wenn man den perfekten diskriminierungsfreien Algorithmus hat, aber eben verzerrte Daten – dann kann das Ergebnis auch nicht diskriminierungsfrei sein. Ich denke, das ist sicherlich in allen Bereichen irgendwie der Fall, weil Algorithmen immer auch – wie ich ja gerade auch gesagt habe – soziotechnische Produkte sind. Aber vor allem bei der Polizei ist das einfach eine ganz wesentliche Frage. Sobald die Polizei mit Algorithmen, mit Datenanalyse-Algorithmen, hantiert, ist einfach die Frage relevant: Was haben wir hier für eine Datenqualität? Wir wissen aus zahlreichen internationalen wie nationalen empirischen Untersuchungen, dass bestimmte Bevölkerungsgruppen, vor allem ethnischer Minderheiten, überrepräsentiert sind in polizeilichen Datenbeständen und letztendlich kann ein Algorithmus, der auf diese Daten zurückgreift, um sich die Welt der Kriminalität zu erschließen, zu keinem anderen Ergebnis kommen, als dass diese überrepräsentierten Bevölkerungsgruppen auch gefährlicher sind. Und da wir wissen, dass diese Überrepräsentanz nicht per se damit zusammenhängt, dass diese Bevölkerungsgruppen tatsächlich gefährlicher sind, sondern mit racial profiling-Praktiken der Polizei zusammenhängen, folgt daraus unmittelbar ein Diskriminierungspotenzial der Anwendung von Algorithmen in der Polizei! Und wenn man das nicht streng monitort und streng darauf achtet, dass wir neutrale und qualitativ hochwertige Datenbestände haben, auf die entsprechende Algorithmen zurückgreifen können, dann führt die Nutzung von Algorithmen innerhalb der Polizei keineswegs per se dazu, dass polizeiliche Tätigkeit diskriminierungsfreier wird.

Zur Frage der Blackbox: Da denke ich, ist es ganz zentral, dass einerseits mit den entsprechenden Firmen vertraglich ganz präzise vereinbart wird, dass Transparenz in maximaler Weise möglich ist, also dass der Algorithmus offengelegt wird und dass es gleichzeitig innerhalb der Polizei – das muss natürlich dann auch sichergestellt werden – dass es da Expertinnen und Experten gibt, die auch in der Lage sind, die entsprechenden Algorithmen, die Codezeilen beispielsweise, zu entschlüsseln, die wirklich für sich selbst und die Kolleginnen und Kollegen, die diese Algorithmen dann benutzen sollen, ganz klar kommunizieren können, was diese Algorithmen können und was eben nicht. Das ist ganz wichtig, dass die Kolleginnen und Kollegen innerhalb der Polizei dann auch adäquat geschult werden – mindestens geschult werden, wenn nicht sogar auch schon im Vorhinein eine substanzielle Aus- oder Weiterbildung erfahren haben –, sodass sie wirklich in der Lage sind, kompetent und kritisch reflexiv diese Algorithmen zu benutzen. Dafür ist es eben notwendig, dass sie hinreichend Transparenz haben. Das ist aus meiner Sicht ganz wichtig, dass das auch vertraglich vorab festgelegt wird, dass es da eine gewisse Einsicht gibt.

Ich möchte noch darauf hinweisen, dass – ich hatte

die Expertinnen und Experten, derer es dann innerhalb der Polizei bedarf, um die Algorithmen auch wirklich zu verstehen. Das deutet noch auf einen Punkt hin, der mir wichtig ist, der hier auch schon erläutert wurde an einigen Stellen von einigen Sachverständigen: Die Digitalisierung der Polizei ist höchst voraussetzungsvoll und eben nicht ein reines IT-Projekt, sondern wirklich ein Projekt, das ein organisationalen Umbruch impliziert. Auch die Organisationskultur ist von der Digitalisierung betroffen. Dazu gehört eben auch, dass das ganze Beförderungsmanagement, also die Generalistenausbildung, die ja bislang weitestgehend gepflegt wird, überdacht werden muss. Und wie es einmal Repräsentanten einer Polizeibehörde, mit denen ich gesprochen habe, so schön gesagt haben: IT-Fachkarrieren innerhalb der Polizei müssen möglich sein, sonst wird die Polizei nicht in der Lage sein, entsprechende IT-Kompetenz auch, gerade in Führungspositionen, aufzubauen, die letztendlich dazu führt, dass solche zum Teil wirklich komplexen Systeme auch adäquat und kompetent reflexiv angewendet werden können. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen nunmehr zu den Antworten von Herrn Gadorosi.

SV **Holger Gadorosi** (Bundeskriminalamt, Wiesbaden): Vielen Dank.

Ich gehe direkt darauf ein – wo stehen wir heute mit dem Programm Polizei 2020 und warum stehen wir da, wo wir stehen? Es ist angeklungen: Saarbrücker Agenda – 30. November 2016 – vor 4 ½ Jahren verabschiedet. Warum stehen wir heute noch relativ am Anfang der Umsetzung und wo liegen die Widrigkeiten?

Die Widrigkeiten liegen nicht so sehr in der IT. Es ist gerade auch angeklungen: Es ist ein Organisationsentwicklungsprojekt, kein reines IT-Projekt. Wir haben die Situation, dass wir – ich habe es eingangs erwähnt – ungefähr 400 Einzelsysteme haben, die wir harmonisieren, die wir vereinheitlichen wollen. Einer der Kollegen hat es auch schon erwähnt: Vereinheitlichung ja, solange es auf mein System ist. Harmonisieren ja, standardisieren ja, solange es meine Standards sind. Das ist ein Problem, das kann man mit IT nicht lösen. Man kann ein System hinstellen, aber es bedingt natürlich die Bereitschaft aller 20 Teilnehmer, sich auch auf diese Standards und Systeme zu einigen. Das ist ein langwieriger Prozess, ich hatte es erwähnt: Polizei ist Ländersache. Es gibt auch nicht denjenigen, der es einfach aufoktroyieren könnte. Das würde auch nichts bringen, es muss ja gelebt werden. Und dieser Prozess hat relativ lange gedauert. Das lässt sich auch daraus ablesen, dass wir Ende 2019 diesen sogenannten IT-Fond eingerichtet haben, über den sich alle 20 Teilnehmer erst dann verständigt haben, wie sie die Programmvorhaben gemeinsam finanzieren wollen, wie die Finanzen zu tragen sind. Wir haben einen Verwaltungsrat mit einer Governance aufgesetzt, mit einer Regelung, die um das Jahresende 2019 verabschiedet wurde. Daran erkennt man, dass die erste Zeit darauf verwendet werden musste, einheitliche Regelungen zu finden, wie wir gemeinsam arbeiten wollen. Es kostet natürlich Zeit, aber a) waren wir in der Zeit nicht tatenlos und b) sind wir seither, glaube ich, auch recht flott unterwegs. Das zeigt sich daran – Herr Schneider hat es erwähnt –, dass aktuell über 30 Projekte in diesem Programm Polizei 2020 behandelt werden. In den 30 Projekten sind auch Bestandssysteme dabei, aber es sind auch ganz neue Ansätze dabei. Nur ein Beispiel: Wir haben mittlerweile nahezu bundesweit eine KI-unterstützte Software eingeführt zur Erkennung kinderpornografischen Materials, damit die Kolleginnen und Kollegen eben nicht die Petabyte Daten händisch ausdrucken oder angucken müssen, sondern eine Vorfilterung stattfindet und die Kolleginnen und Kollegen sich mit dem leider relevanten Material beschäftigen können und nicht ihre Zeit mit irrelevantem Material verschwenden. Das sind Systeme, die bereits eingeführt sind. Wir haben andere Wirkbetriebsaufnahmen bereits durchgeführt, in anderen Themenfeldern, und wir sind in der operativen

Umsetzung weiterer Fehlersysteme. Und wir sind natürlich auch bei dem einen oder anderen System noch in der Anlaufphase. Aber die Widrigkeiten beruhen, wie gesagt, stärker auf dem ganzen organisatorischen Umfeld. Dafür haben wir auch ein Change-Management im Programm etabliert, welches die Kolleginnen und Kollegen – wir reden immerhin von circa 300.000 Polizistinnen und Polizisten deutschlandweit im Alter von 16 bis plus minus 60 Jahren – also eine recht breite Spanne, was das Thema Digitalisierung betrifft – entsprechend mitnehmen soll.

Des Weiteren steht ganz klar die Mobilität der Nutzer bei der technischen Umsetzung der Lösungen im Mittelpunkt. Wir haben eine IT-Strategie „Mobilität“ aufgesetzt, sodass wir zukünftig Smartphones, Tablets, Car PCs, was alles schon erwähnt wurde, auch entsprechend mit einbinden und nutzen können – auch bundesweit übergreifend nutzen können, nicht nur auf einer Teilnehmerseite, sondern so, dass auch in größeren Lagen die Zusammenarbeit gewährleistet ist, sowohl innerhalb der Bundesrepublik als auch international Richtung EUROPOL, INTERPOL. Die sind da auch alle mit berücksichtigt bei diesem Programm Polizei 2020.

Wie sieht die konkrete Planung aus, wie sehen unsere Zielvorstellungen aus? Es wird nicht den Big Bang geben, wo wir sagen, „jetzt sind alle 400 Systeme abgebildet und jetzt legen wir den Schalter um“, sondern wir gehen schrittweise vor. Wir nehmen uns einzelne Systeme vor und lösen die ab. Bei den operativen polizeilichen Kernsystemen oder Kernanwendungen der polizeilichen Sachbearbeitung und der Verbundsysteme haben wir eine Planung aufgesetzt, dass wir bis Ende 2028 über 100 dieser 400 Systeme vereinheitlicht/harmonisiert und auch bundesweit abgelöst und eingeführt haben wollen. Also Ende 2028 werden in diesem polizeilichen Kernarbeitsbereich alle Kolleginnen und Kollegen mit einheitlichen Systemen, auf einer einheitlichen Datenbasis arbeiten. Auf dem Weg dorthin wird es entsprechende Synchronisationspunkte geben und werden viele parallele Projekte vorangetrieben. Ich hatte erwähnt, über 30 Projekte laufen, wir machen vierteljährlich sogenannte Synchronisationsmeetings, wo sich 150 Kolleginnen und Kollegen zwei bis drei Tage zusammenschalten, um diese 30 Projekte so aufeinander abzustimmen, dass zu jeder Millisekunde in dieser Republik die Handlungsfähigkeit der Polizei gewährleistet ist und dass wir nicht einmal eine Woche oder auch nicht nur eine Sekunde oder einen Tag die Systeme runterfahren und ausschalten müssen, weil wir uns nicht ordentlich abgestimmt und synchronisiert haben. Das ist viel Aufwand, den man sich sparen könnte, wenn wir auf der grünen Wiese unterwegs wären. Das sind wir nicht, das wissen wir auch und der Aufwand ist gut investiert. Es braucht aber dann eben auch ein bisschen Zeit, die Systeme – die ganze Bandbreite, die erwähnt wurde: Datenschutzregelungen, gesetzliche Regelungen aber auch polizeiliche Handlungsfähigkeit, die Funktionalität, die einfach notwendig ist und die sich gewandelt hat im Laufe der letzten Jahrzehnte – umzusetzen. Wir haben heute eine Systemlandschaft, die auf das Herold’sche RAF-Bild zurückgeht in den 70er Jahren. Das ist immer noch die grundlegende Systemlandschaft, wie wir in der Republik die IT-Systeme organisiert haben und wie die Polizeiarbeit auch weitestgehend funktioniert. Die ist der Aufgabenstellung nicht mehr angemessen, die ist nicht mehr adäquat. Die wollen, die müssen wir überwinden. Wir brauchen viel flexiblere Systeme – und ja, da gibt es datenschutzrechtliche Risiken. Die sind uns auch bewusst, da sind wir auch im engen Austausch mit den Datenschützern. Die sind aber aus meiner Sicht beherrschbar und die Systeme, die wir derzeit einführen, die werden in Abstimmung mit den Datenschützern – nach heftigen Diskussionen – dann auch an den Start gebracht und eingeführt. Wir werden auch die neue Systemwelt, die wirklich ganz andere Möglichkeiten eröffnen wird, mit den Datenschützern gemeinsam einführen. Ob es Rechtsetzungsbedarf gibt, weiß ich nicht, werden wir sehen. Ist aber in der Planung auch

soweit berücksichtigt, dass, wenn es notwendig werden würde, wir dann entsprechend aktiv werden können. Das Programm ist umfangreich aufgestellt und berücksichtigt diese Aspekte entsprechend.

Auf die zweite Frage – das „Homeoffice für alle“: Ja, es gibt diese Mobilstrategie, die wir uns im Programm gegeben haben. Da wird geprüft, welche Smartphones – wie müssen die Anwendungen der Zukunft aussehen, dass sie auf einem breiten Spektrum an Smartphones, an Tablets, an marktgängigen Systemen funktionieren. Die Nichtnutzung des Digitalfunks mit derzeit gängigen Smartphones – das ist allseits bekannt. In die Lücke wollen wir natürlich nicht rennen, sondern wir wollen auf Standardprodukte setzen. Der Markt ist nicht groß genug, dass wir eigene Smartphones oder ähnliches für die Polizei entwickeln oder anschaffen sollten, sondern es müssen Standardprodukte sein. Die werden wir auch entsprechend unterstützen – da ist ein ganz großer Fokus darauf.

Auch das Thema Messenger-Lösungen, dass die Messenger gemeinsam miteinander funktionieren und interagieren können – da sind wir bereits dran. Da gibt es auch schon erste teilnehmerübergreifende Aufgaben oder Problemlösungen, wo der ein oder andere Teilnehmer trotz unterschiedlicher Messenger-Lösungen miteinander kommunizieren kann. Also es ist ein ganz großes Themenspektrum bei uns. Natürlich durch die Pandemie noch angeheizt. Egal ob es Laptop, Smartphone, Car PC oder ähnliche zukünftige mobile Endgeräte sind – die stehen bei uns im Fokus und werden auch entsprechend berücksichtigt.

Zum Organisationsthema vielleicht auch noch einmal: Auch da hat die Bundesregierung, denke ich, reagiert. Wir haben bei der BAKÖV eine sogenannte Digitalakademie eingerichtet. Dort werden digitale Fähigkeiten auch polizeiunspezifisch vermittelt. Bei uns im Programm Polizei 2020 ist es natürlich ein Stück weit Ländersache, die Kolleginnen und Kollegen mitzunehmen. Auch da haben wir eine große Gruppe eingerichtet, die sich zum einen um das ganze Thema der Transparenz und Öffentlichkeitsarbeit nach innen kümmert, aber eben auch um das ganze Thema Change-Management – die Kolleginnen und Kollegen mitnehmen, die Ängste abbauen und die Kolleginnen und Kollegen befähigen, die Systeme zu nutzen. Ich habe zum Beispiel heute Mittag einen Termin mit der Polizeihochschule in Münster, wo wir auch die nächsten Schritte besprechen werden, wie wir diesen ganzen Aspekt stärker in die polizeiliche Ausbildung einbinden. Soweit von meiner Seite. Danke schön.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zu den Antworten von Herrn Michelfelder.

SV **Ralf Michelfelder** (Landeskriminalamt Baden-Württemberg): Die erste Frage betraf künstliche Intelligenz für Polizeibehörden – Herr Gadorosi hat da schon Beispiele erwähnt, wie die Auswertung von belastendem Kinderpornografie-Material. In Baden-Württemberg läuft im Moment ein Projekt zur Erkennung von Falschidentitäten, falschen Ausweispapieren. Experten sagen, es gibt in Europa so viele falsche Ausweispapiere im Umlauf, wie Italien Einwohner hat. Um so etwas dann schnell erkennen zu können, bedarf es entsprechender selbstlernender Systeme, die aus Erfahrungen lernen und Ausweisfälschungen sicher erkennen und dann auch bereits teilautomatisierte Gutachten erstellen können. Teilautomatisiert heißt – und da bin ich bei Herrn Professor Aden – dass nachher noch ein echter Gutachter draufschaut und dieser dann das vom System vorgeschlagene Gutachten verifiziert. Bayern engagiert sich beispielsweise im Moment stark im Bereich der Gesichtserkennung, einer Software zur Erkennung von Tatverdächtigen, auch nur mit Teilen des Gesichtsfeldes und offenen Gesichtsfeldern. Die haben letztes Jahr circa 650 Identifizierungen auf diese Weise durchgeführt, 2013 waren es noch 45 – da tut sich Einiges. Aber Bedingungen ist natürlich, dass die Systeme dann nicht isoliert in einzelnen Bundesländern stehen bleiben, sondern auch anderen Bundesländern zur

Verfügung gestellt werden, wie es ja Polizei 2020 vorsieht.

Probleme sind aus meiner Sicht die Zeitläufe. An was die liegen, hat Herr Gadorosi dargestellt, aber das interessiert im Zweifelsfall die Staatsanwaltschaft wenig. Wenn wir denn ein großes Ermittlungsverfahren haben mit Haftsachen, dann müssen die Daten jetzt ausgewertet werden und nicht später mit Hinweis darauf, dass wir in ein, zwei Jahren irgendwie eine Auswertesoftware haben, die das dann schneller hinbekommt. Aus meiner Praxis kann ich sagen, wenn ich ein Wirtschaftsstrafverfahren habe, wo die Tat schon erfolgt ist und es im Grunde um den Tatnachweis geht und ich habe andererseits eine Durchsuchungsmaßnahme bei islamistischen Gewalttätern, wo ich nicht weiß, ob ein Anschlag vorbereitet wurde, dann stelle ich das eine zurück und lasse das auswerten, was mir im Moment mehr unter den Nägeln brennt. Für mich wäre der GAU, dass wir eine Anschlagsvorbereitung in den Daten haben, sie aber nicht rechtzeitig erkennen. Und diesen Zwiespalt aufzulösen, ist angesichts unzureichender IT-Systeme extrem schwierig. Also man kann entweder das eine machen oder das andere, aber man kann oftmals nicht beides gleichzeitig machen. Das führt dann im Zweifelsfall zu Fremdvergaben durch die Beauftragung der Staatsanwaltschaft – aus meiner Sicht eine ganz kritische Angelegenheit. Erstens ist dann das Geld weg. Wir hatten einmal eine Fremdvergabe in einem Verfahren bei uns, das war ein großer sechsstelliger Bereich an Kosten, die wir für unsere Systeme hätten besser einsetzen können. Zum Zweiten ist Ihnen sicherlich auch gegenwärtig der Fremdvergabe-Skandal in Hessen, wo letzten Endes ein hochrangiger Staatsanwalt in Haft genommen wurde, wegen Cashback-Zahlungen von dem Gutachter zurück an den Staatsanwalt. Und jetzt sage ich – nicht auf dieses Verfahren bezogen – aber generell: Wenn schon die Auftragsvergabe manipulativ verlaufen kann, wie ist das dann mit den Ergebnissen? Und von daher ist für mich wichtig, dass diese Auswertungen in der Polizei erfolgen, mit Systemen der Polizei.

Wir haben die meisten Daten, die uns immer mehr erdrücken und die sicherlich nicht weniger werden. Und ich glaube, wir werden mit Polizei 2020 nicht den Zeitpunkt haben, wo wir sagen: „Alles ist erledigt.“, sondern es gibt ständig neue Herausforderungen. Wir müssen auf diese neuen Herausforderungen wieder neu reagieren, möglichst zeitnah, sonst entstehen diese Parallelbeschaffungen. Diese Parallelsysteme entstehen nicht, um Polizei 2020 ans Schienbein zu treten, sondern die entstehen einfach aus dem Zeitdruck, der sich aus den Ermittlungen ergibt.

Was die Fortbildung betrifft, muss man meiner Ansicht nach differenzieren zwischen Grundwissen, das heutzutage jeder Polizeibeamte braucht. Als ich seinerzeit ausgebildet wurde, hat man uns noch erklärt, welche Spuren man bei einem Wohnungseinbruch zu erwarten hat, welche Werkzeugspuren, welche Fingerspuren, welche Fußspuren, wie man die zu sichern hat und wo man gegebenenfalls etwas kaputt macht, wenn man sich falsch am Tatort bewegt. Heutzutage muss man wissen, wenn ich ein sogenanntes Smart Home habe: Kann der Kollege überhaupt die Tür öffnen oder das Licht an- und ausschalten? Oder überschreibt er damit Datensätze im System, die nachher für die Tataufklärung und für den Tatzeitraum von Relevanz wären? Er muss sich darüber im Klaren sein, wo sind diese im Grunde unsichtbaren Spuren, die ich zum einen sichern kann, aber die ich im Zweifelsfall auch zerstören kann? Und dieses Grundwissen braucht jeder. Und dieses Grundwissen muss in der Ausbildung verankert werden. Die Lehrpläne müssen umgeschrieben werden, nicht nur Cyberspezialisten eigene Lehrpläne schaffen, sondern Grundwissen für jede Kollegin und jeden Kollegen.

Expertenwissen ist das Zweite: Wir brauchen natürlich Leute – ich habe vorhin einmal den Begriff erwähnt: „Datenanalysten“ oder „Intelligence Analyst“, die mit leistungsstarken Systemen, mit leistungsstarker Software, auch das

rausholen können, was diese Software bieten kann und sich nicht nur an der Oberfläche bewegen. Auch da sind wir in Baden-Württemberg dabei, die Ausbildungspläne anzupassen: Es wird einen eigenen Studiengang „Cyber-Kriminalist“ bei der Hochschule für Polizei in Baden-Württemberg geben. Aber das wird nicht reichen. Angesichts der Durchdringung der Gesellschaft mit Digitalisierung brauchen wir da eine Masse an Leuten, die sich mit solchen Systemen auskennen. Also wir brauchen externe Unterstützung durch die Einstellung von Datenanalysten, die der Markt so aber gar nicht hergibt.

Dann sehen wir es mittlerweile auch so, dass wir sagen, die Abwanderung von Kolleginnen und Kollegen und der Wettbewerb ist hier groß, also der Bedarf an IT-Forensikern ist nicht nur in der in der Polizei groß, sondern auch in der freien Wirtschaft, bei Versicherungsunternehmen oder wo auch immer. Abwanderung müssen wir als Chance sehen, nicht als Risiko. Israel ist heutzutage weltmarktführend im Bereich der Cyber-Sicherheit. Das hängt sicherlich auch damit zusammen, dass Israel noch immer eine Wehrpflicht mit drei Jahren für Männer und zwei für Frauen hat, mit speziellen Cyber-Einheiten. Und wenn man die Fähigkeiten hat und die Grundanlagen, dann wird man in so einer Cyber-Einheit den Dienst verrichten und nach drei Jahren die Armee verlassen mit einem Wissen, dass auf dem freien Markt nachgefragt ist. Und diese Leute gründen dann Unternehmen oder werden Teil eines Unternehmens und lösen dort Probleme, von denen die Firma im Zweifelsfall noch gar nicht weiß, dass sie sie hat. Wir gehen jetzt in Baden-Württemberg den Weg, dass wir ein duales Studium einrichten an der dualen Hochschule Baden-Württemberg, zusammen mit den großen Industrieunternehmen und beiderseits Studienplätze anbieten mit gegenseitiger Hospitation. Die Studierenden, die über diese Firma eingestellt sind, hospitieren bei der Polizei und unsere jungen, einzustellenden Kollegen, werden dann bei dieser Firma hospitieren. Wir müssen uns mehr vernetzen und wir müssen gegenseitig einen höheren Austausch pflegen, was im Grunde dann auch dazu führt, dass das Vertrauen in die Kompetenzen der Polizei im Bereich Cyber-Ermittlungen auch in der Wirtschaft gestärkt wird. Soweit unsere Ansätze dazu. Es wird aber keine Kurzstrecke, sondern ein Marathon! Danke.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen nunmehr zu den Antworten von Herrn Schneider.

SV **Dieter Schneider** (Landeskriminalamt Baden-Württemberg): Vielen Dank für die Fragen, Herr Müller.

Digitales Leitbild für die Polizei und Digitalpakt hängen ja schon ein bisschen zusammen. Bestehen hier weitere Notwendigkeiten? Greifen wir zeitlich auf eine Phase vor die Saarbrücker Agenda zurück: Wir haben Ansatzpunkte und Ausführungen zur digitalen Ausgestaltung der Polizeiarbeit bereits im Programm für die Innere Sicherheit als übergelagertes Leitbild oder, wenn Sie so wollen, als Digitalpakt, jedenfalls in dem entsprechenden Abschnitt. Man muss sich immer fragen bei einem solchen Leitbild für die Polizei: Wer ist denn Adressat und Zielgruppe? Es ist schon angeklungen, die 250.000 Kollegen vor Ort, die interessiert es nicht, ob es hier einen Digitalpakt oder ein Leitbild gibt, sondern die wollen funktionierende Systeme haben – so, wie sie es im Alltag gewohnt sind – will sagen: Ob da noch einmal eine Hochglanz-Broschüre erstellt wird mit einem solchen Label oder nicht, hat relativ wenig Auswirkung auf die praktische Polizeiarbeit! Trotzdem – ich will das nicht verkennen und auch bestätigen – hat natürlich ein solches Positionspapier Auswirkungen auf die Realisierung von umzusetzenden Bestandteilen in der digitalen Welt.

Solche Grundsatzpapiere haben nach eigenen Erfahrungen einen sehr, sehr langen Weg. Die Erfahrungen aus dem Programm für Innere Sicherheit zeigen, wie viele Jahre gearbeitet wurde und wie um jedes Wort und Komma gerungen wird, um den kleinsten gemeinsamen Nenner als Kompro-

miss zu finden. Und das muss man sich vor Augen führen, wenn man die Frage stellt: Brauchen wir noch einmal ein übergelagertes oder ein neues Leitbild oder einen neuen Digitalpakt? Ich finde die Aussagen, insbesondere in der Saarbrücker Agenda, mit den komprimierten Leitlinien, auf die man sich in relativ kurzer Zeit – jedenfalls politisch auf der ministerialen Ebene – verständigt hat, geben schon die Richtung vor – plakativ und umsetzungsrelevant. Ich zitiere einfach einmal eine Passage: „Die zukünftige IT der Polizei ist einfach und anwenderfreundlich.“ Also da steckt schon richtig viel drin, jedes Wort ein Pfund! „Sie wird kontinuierlich dem jeweiligen Stand der Technik und den Anforderungen der IT-Sicherheit angepasst. Polizeiliche IT-Angebote, die Bund und Länder gleichermaßen betreffen können, werden nur einmal entwickelt und stehen allen Bedarfsträgern in den Ländern zur Verfügung.“ So zieht sich das durch in dieser Saarbrücker Agenda. Komprimiert, schwergewichtig und meines Erachtens im Sinne eines Leitbildes aussagekräftig – im Programm selbst, aber auch in Umfeld-Vorhaben, die außerhalb des Programmes Polizei 2020 bei den Teilnehmern laufen, von Bedeutung. Als Orientierungsrichtschnur ist das aus meiner Sicht gut gelungen. Ob ein zweiter Anlauf die ein- oder andere Akzentverschiebung bringen würde, darüber kann man trefflich streiten, aber die Grundzüge stehen damit, glaube ich, sehr gut fest und sind für die Umsetzung geeignet. Und zwar in Bund und Ländern in diesem föderalen Spannungsfeld.

Den Digitalpakt würde ich noch einmal aus der Perspektive der Rechtsverbindlichkeit oder der Verbindlichkeit beleuchten wollen: In den verschiedenen Gremien, die sich letztendlich mit der Umsetzung der Saarbrücker Agenda beschäftigt haben – das waren parallele Stränge – hat man über die Entwicklung hin zum IT-Fonds versucht, sich auf ganz unterschiedlichen Wegen zu nähern. Da stand natürlich im Raum: Machen wir einen Staatsvertrag, also so etwas Ähnliches wie den Digitalpakt? Da stand im Raum: Verständigen wir uns auf eine behördliche Struktur zur Umsetzung? Also beispielsweise eine Anstalt des Öffentlichen Rechts, wie wir es im Digitalfunk haben? Da stand im Raum: Schließen wir uns mit einer Verwaltungsvereinbarung zusammen? Die Abwägung dieser drei und vielleicht noch weiterer Möglichkeiten hat dann dazu geführt, dass man sich dieser Verwaltungsvereinbarung bedient hat. Die Ausarbeitung eines Staatsvertrages, der von 16 Länderparlamenten zu ratifizieren gewesen wäre – wir hätten ihn heute noch nicht, da braucht man kein Prophet sein. Also der Weg pragmatisch und dennoch mit der möglichen, umsetzbaren Konsequenz. Einen solchen „Pakt“ zu beschließen, ist, glaube ich, mit der Vereinbarung des IT-Fonds durchaus gut gelungen und man darf ja nicht verkennen, dieser IT-Fonds ist ja in einigen Ländern auch parlamentarisch gebilligt worden und wird ja nicht nur von der Innenministerkonferenz sondern auch von der Finanzministerkonferenz getragen und hat damit eine hohe Verbindlichkeit. Natürlich, aber das wäre auch bei einem Digitalpakt formeller Art/staatsvertraglicher Art nicht anders, mit dem Haushaltsvorbehalt, das heißt, dass von Haushaltsperiode zu Haushaltsperiode zu verhandeln ist, welche Budgets zur Verfügung gestellt werden. Aber der Grundsatz, die Umsetzung dieses IT-Fonds mit den dort festgelegten Regularien, der steht. Also ich halte sowohl ein neues, zusätzliches digitales Leitbild als auch einen Digitalpakt in formalisierter, staatsvertraglicher Form nicht für erforderlich.

Zu der Frage, Herr Hess, Eingangsstatistik über Migrationshintergründe, Aufenthaltsstatus, so habe ich es verstanden, ausgehend von den Einsätzen in Stuttgart mit dem Stichwort „Partyszene“. Ich frage mich bei der Eingangsstatistik: Was soll eine solche bringen, jedenfalls für die polizeiliche Arbeit? Richtig ist, und das wird ja auch gemacht, dass bei den Ermittlungen – soweit es für die Aufhellung der Straftat und der Täterpersönlichkeit, soweit sie Tatrelevanz hat, erforderlich ist – aufgeklärt wird, welchen sozialen/persönlichen Hintergrund die Tatverdächtigen haben. Das gehört zum Hand-

werkszeug dazu. Und wenn das relevant ist für die Straftatenaufklärung und die Beurteilung der Täterpersönlichkeit für das nachfolgende gerichtliche Strafverfahren, dann werden auch Aspekte der Herkunft, des sozialen Umfeldes und damit auch des Migrationshintergrundes beleuchtet und in das Verfahren mit eingebracht. Das ist das, was die Polizeibeamtinnen und Polizeibeamten vor Ort tun. Eine eingangsstatistische Erfassung, weiß ich nicht, was die darüber hinaus für die Polizeiarbeit bringen sollte.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir jetzt zur zweiten Fragerunde und beginnen wieder bei der CDU/CSU-Fraktion und Herrn Müller.

BE Abg. **Axel Müller** (CDU/CSU): Ich mache es kurz: Ich hätte noch eine Frage an Sie, Herr Schneider. Und zwar sind in dem Antrag ja auch die Messenger-Dienste explizit aufgeführt. Mich würde interessieren, welche Bedeutung haben denn die mobilen Anwendungsbereiche wie Messenger oder WhatsApp und so weiter und so fort in der derzeitigen digitalen Aufarbeitung?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Keine Fragen bei der AfD-Fraktion? SPD-Fraktion, Frau Mittag?

BEin Abg. **Susanne Mittag** (SPD): Ich hätte an Herrn Gadorosi noch einmal eine ergänzende Frage. Es geht ja nicht nur um die Anpassung von Systemen, sondern auch um die Anpassung von Begrifflichkeiten. Ich erinnere da an die Debatte, die wir vor einer ganzen Weile hatten: Was ist zum Beispiel die Legaldefinition für einen „Gefährder“? Da hatten 16 Bundesländer offensichtlich 16 verschiedene Auffassungen – das ist angepasst worden, aber das haben wir hier ja noch. Wie viele Begrifflichkeiten haben wir, gerade in dieser statistischen Erfassung? Ich glaube, das sind nicht wenige. Werden die Begrifflichkeiten noch angefasst, wenn sozusagen bundesweit und auf Bundesebene identisch eingegeben werden muss? Das muss ja auch noch umtrainiert und definiert werden. Und hat das dann am Ende auch eine Auswirkung auf die Statistik? Wir haben ja noch immer eine Debatte über die Vorlage eines periodischen Sicherheitsberichtes. Es geht nicht nur darum, nach hinten zu gucken – was ist passiert? – sondern eben auch darum, vor die Lage zu kommen. In welchem Rahmen kann das zum Erkenntnisgewinn führen, wie sich Kriminalität entwickelt, um besser vorher zu reagieren, nicht nur bei Prävention, sondern auch bei polizeilichen Maßnahmen?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zur FDP-Fraktion und Herrn Strasser.

BE Abg. **Benjamin Strasser** (FDP): Vielen Dank.

Vielleicht vorweg noch einmal zur Klarstellung: In unserem Antrag steht keine Homeoffice-Pflicht für alle, sondern dass man die Voraussetzungen für Homeoffice schaffen soll bei den Tätigkeiten, wo es mit dem Charakter der Tätigkeit vereinbar ist. Das ist etwas anderes und es ist eine bloße Selbstverständlichkeit, wenn ich wie die SPD von der deutschen Wirtschaft eine Homeoffice-Pflicht fordere, dass ich dann vielleicht als Staat zumindest als gutes Beispiel vorangehe.

Meine Fragen zum einen an Herrn Michelfelder: Sie waren ja selbst als aktiver Präsident des Landeskriminalamtes begleitend in der Umsetzung der Saarbrücker Agenda dabei. Wenn Sie die Saarbrücker Agenda selbst hätten schreiben dürfen, was hätten Sie denn hineingeschrieben, beziehungsweise was fehlt, was aus Ihrer Sicht erforderlich ist?

Und die zweite Frage ist eine ganz spannende Frage: Wenn wir feststellen, dass Polizei 2020 ein Prozess ist, der nicht abgeschlossen ist, dass auch die Themen Software-Entwicklung, Messenger-Lösungen oder sonstiges kein Prozess ist, der 2028 abgeschlossen sein wird, sondern ein kontinuierlicher Prozess bleibt – und Sie haben ja auch gesagt, Herr Michelfelder, warum denn unterschiedliche Messenger-Lösungen erarbeitet werden:

weil man es einfach jetzt braucht und nicht erst in zwei Jahren. Brauchen wir dann nicht auch organisatorisch eine verpflichtende Verständigung zwischen Bund und Ländern für künftige Software-Entwicklungen? Nicht status quo, wie es Herr Schneider dargestellt hat, einfach gerade deshalb, weil es unkomplizierter ging. Aber die Verbindlichkeit für die Zukunft – brauchen wir nicht hier wirklich einen Digitalpakt, einen Staatsvertrag, wo Bund und Länder auch verbindlich vereinbaren, wie man zukünftig mit Entwicklungen von Software innerhalb der deutschen Polizei umgeht?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zur Fraktion DIE LINKE. und Frau Pau.

BEin Abg. **Petra Pau** (DIE LINKE.): Danke! Herr Egbert, ich habe noch eine Frage an Sie: Sie haben sowohl in Ihrer schriftlichen Stellungnahme sehr ausführlich und plastisch auf die Risiken zum Thema Überwachung hingewiesen und haben das vorhin auch ausgeführt. Ich wüsste gern von Ihnen, wie aus Ihrer Sicht die dahinter stehende Dynamik gebrochen werden kann? Reicht es aus, einer solchen Analyse-Software nur den Zugriff auf ohnehin vorhandene polizeiliche Daten zu gestatten oder müssten wir hier noch weitere Beschränkungen vornehmen? Das stellt natürlich noch weitere Fragen einerseits an den Gesetzgeber, aber es ist natürlich auch schon die Frage, wenn Aufträge ausgelöst werden, beziehungsweise wenn wir beschreiben, was wir eigentlich haben wollen und das entsprechend weiter entwickeln? Also ich wüsste gern, wie man gegen diese Risiken und Nebenwirkungen von vornherein auch präventiv vorgehen kann.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zum BÜNDNIS 90/DIE GRÜNEN und Frau Dr. Mihalic.

BEin Abg. **Dr. Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, ich habe auch noch zwei Fragen an Professor Aden. Zum einen auch noch einmal zu den Messenger-Diensten: Da würde mich konkret interessieren, wie Sie die Forderung der FDP bewerten, auch die Möglichkeit zur Kommunikation über eingestufte Sachverhalte über Messenger-Dienste für die Polizei zu schaffen.

Und dann habe ich noch eine letzte Frage: Sie haben ja auch in Ihrer schriftlichen Stellungnahme viel über die Chancen und Risiken der Digitalisierung bei der Polizei geschrieben und hier ja auch ausgeführt und da würde mich interessieren, ob Sie internationale Beispiele für eine erfolgreiche Digitalisierung der Polizei kennen bei gleichzeitig rechtsstaatlich hohen Standards? Und können daraus für Deutschland Schlussfolgerungen gezogen werden?

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zur zweiten Antwortrunde, die wir traditionell in umgekehrt alphabetischer Reihenfolge begehen, sodass wir mit Herrn Schneider beginnen.

SV **Dieter Schneider** (Landeskriminalamt Baden-Württemberg): Vielen Dank und vielen Dank auch noch einmal für die Frage, inwieweit die Messenger-Dienste bei den aktuellen Arbeiten an der gemeinsamen digitalen Strategie Berücksichtigung finden. Das ist ein Thema, wo die Praxis die Polizeiführungen und die politischen Führungen in den Ländern gezwungen hat, schnell zu agieren. Wir haben in nahezu allen Ländern, glaube ich, die gleiche Situation gehabt, dass im Alltag die Polizistinnen und Polizisten ihr privates Handy mitführen und mangels der Zurverfügungstellung vergleichbarer dienstlicher mobiler Geräte über ihr privates Device kommunizieren, Bilder austauschen, Informationen weiterleiten, welcher Art auch immer, weil die IT-Ausstattung mit vergleichbarer Hardware nicht gegeben war. Daraus entsteht ein nachvollziehbarer Druck, da liegen Gefahren – die Nutzung privater Geräte für dienstliche Zwecke – die man nicht haben will. Und daraus ist in allen – mir ist keine Ausnahme bekannt – Ländern dieser Republik die Einführung von Smartphones und vergleichbaren mobilen Devices initiiert worden – mit Einzellösungen zur dienstlichen Kommunikation, teilweise mit Abfragemöglichkeiten des

Fahndungsbestandes und Möglichkeiten, Daten für die Unfall- oder Anzeigenaufnahme zu erfassen. Das ließ sich nicht bündeln in einer gemeinsam konzertierten Aktion eines bundesweiten Vorgehens.

Die Situation haben wir. Und nun wird es darum gehen, aus dieser wiederum sehr heterogenen Landschaft die Harmonisierung und Konsolidierung zu betreiben. Das wird in diesem Feld, glaube ich, noch schwieriger als in dem allgemeinen Feld der informationstechnischen Zusammenarbeit – jeder hat hier sein eigenes Konzept, seine eigene Hardware-Ausstattung, seine eigene Philosophie – was ermögliche ich unter welchen Voraussetzungen mit diesen mobilen Devices? – und dann natürlich auch die konzeptionell grundsätzliche Frage: Was wickle ich über die Messenger-Dienste ab, was wickle ich über den Digitalfunk ab? Wir dürfen den Digitalfunk nicht abschreiben, wir brauchen die Digitalfunk-Kommunikation.

Wer polizeiliche Arbeit kennt, der weiß, ich muss Einheiten führen, Einsätze koordinieren – wie bekomme ich diese Zusammenführung von Digitalfunk-Kommunikation und Messenger-Kommunikation zusammenwirkend sinnvoll geregelt? Also das hört sich jetzt einfach an, man macht einen einheitlichen bundesweiten Messenger und dann haben ihr es, aber hier steckt der Teufel im Detail – oder auch schon in den Grundzügen: Die einen wollen die Verknüpfung von Digitalfunk und Messenger-Diensten, die anderen haben die Trennung; die einen wollen es integriert im Fahrzeug haben, die anderen setzen auf Mann-Ausstattung. Die Fahrzeuge wechseln in Leasingverfahren alle zwei oder vier Jahre – da kann ich nichts Zusätzliches einbauen. Im Übrigen ist das Fahrzeug allein schon ein rollender Computer. Und da noch unsere Technik mit zu verbauen, über die dann möglicherweise VS-Kommunikation abläuft, ohne die Kommunikation mit dem Fahrzeug herzustellen – also da stellen sich Fragen über Fragen. Und deshalb wird dieses Problem eines bundesweiten Polizei-Messengers kurzfristig nicht zu lösen sein. Wir haben schon lange in der Polizei über die Kommunikation der Spezialeinheiten gerungen. Da haben wir eine Lösung für diesen kleinen Kreis, aber für die breite Anwendung wird das, glaube ich noch sehr, sehr lange dauern.

Was tut man, um diese Problematik voranzubringen? Wir haben zum einen das Vorhaben „Mobilstrategie“ im Programm Polizei 2020 implementiert, das sich im Moment in der Anlaufphase befindet und das insbesondere auch die Verknüpfung mit einer neuen Breitbandstrategie des Digitalfunks herzustellen hat. Also: Nutzen wir die herkömmlichen Möglichkeiten der klassischen Anbieter? Oder setzen wir eher auf ein eigenes Kernnetz im Zusammenhang mit der Breitbandstrategie? Es bleibt noch so viel zu erarbeiten, dass ich Ihnen keine Illusionen wecken möchte, dass wir hier eine schnelle Lösung haben. Und gleichzeitig haben wir vor Ort – ich sage nochmal, was ich eingangs schon gesagt habe – den Druck aus der Fachlichkeit, aus den Anwendern, schnelle Lösungen zur Verfügung zu stellen und uns zu trennen vom Einsatz privater Smartphones oder anderen privaten Mobile Devices, um hier auch einigermaßen die Sicherheit der Kommunikation zu gewährleisten.

Will sagen: man ist dran. Es gibt auch dazu Bund-Länder-Arbeitsgruppen, auch außerhalb des Programms, die sich mit dieser Frage beschäftigen, aber das wird im Föderalismus ein ganz, ganz dickes Brett werden – ich bin überzeugter Föderalist, sage dies aber trotzdem an der Stelle so deutlich!

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir zu den Antworten von Herrn Michelfelder.

SV **Ralf Michelfelder** (Landeskriminalamt Baden-Württemberg): Danke.

Also zuerst einmal großen Respekt dafür, dass es die Saarbrücker Agenda überhaupt gibt. Für jeden

Polizeipraktiker war das ein Schritt nach vorn, dass so etwas gelungen ist, dass man sich auf diese Grundsätze geeinigt hat: Einer entwickelt, alle nutzen es, gleiche Systeme im ganzen Bundesgebiet – das darf man wirklich nicht geringschätzen.

Natürlich gibt es immer etwas, was man noch gern zusätzlich hätte und was besser werden würde, wenn… Wenn Sie mich nach meinen Wünschen fragen, Herr Strasser: Wir sprechen ja hier von nationaler Sicherheit. Und für mich wäre es wichtig, ein Verfahren zu implementieren, wo man sagt: Weg von herkömmlichen Beschaffungen! Hier geht es um dringliche Bedarfe, hier brennt es unter den Nägeln. Über die Themen, die im Bereich von Polizei 2020 jeden Tag erörtert werden: Da, da und da geht es nicht, weil das ist was – ich habe es vorhin schon einmal angesprochen –, was fünf Jahre dauert. Wir haben in Baden-Württemberg das Asservatenmanagementsystem eingeführt – im Sinne der Saarbrücker Agenda auch für alle Bundesländer. Das läuft jetzt im Pilotbetrieb. Nach fünf Jahren! Zweieinhalb Jahre davon waren Vergabeverfahren! Meines Wissens sollte ein Generalunternehmen für Polizei 2020 beauftragt werden, auch da rechnet man mit zweieinhalb Jahren Vergabeverfahren. Das sind Abläufe, die man sich im Bereich der nationalen Sicherheit meines Erachtens nicht leisten kann. Da muss es andere Lösungen geben, dass wir schneller zum Ergebnis kommen. Dazu gehört für mich letzten Endes auch die Verpflichtung, Produkte von der Stange zu kaufen und jeder hat die zu nutzen. Herr Gadorosi hat das auch angeführt: Jeder findet, seines ist das Beste. Man muss sich darauf einigen, dass es letzten Endes sowieso bei jedem passiert, wenn er sein Landessystem ändert in ein anderes Vorgangsbearbeitungssystem oder was auch immer, dass es dann neue Applikationen gibt, die sinnvoll sind oder man andere schmerzlich vermisst – da muss man halt durch. Das hat jeder zu akzeptieren und deshalb wäre für mich ein Thema, Standardprodukte zu nehmen und nicht mehr so viel in eigene Entwicklungen zu investieren.

Föderalismus – Herr Schneider hat es angesprochen: Föderalismus ist gut für die Polizeiarbeit, wenn man sich auch an den regionalen Schwerpunkten orientieren kann, ist aber schwierig für die Beschaffung – in allen Bereichen. Und das zeigt sich im IT-Bereich ganz besonders.

Bevor ich zu den Messengern komme: Mir müssten im Bereich der Saarbrücker Agenda mehr auch noch die polizeilichen Partner einbeziehen, also sprich die Staatsanwaltschaften. Was brauchen die von uns? Was erwarten die von den polizeilichen Produkten? Und wir werden im Bereich der Daten meines Erachtens nicht umhin können, dass wir irgendwann einmal mit den Staatsanwaltschaften einigen, was wird überhaupt noch ausgewertet und was nicht? Ich habe vorhin ein Beispiel genommen aus dem Bereich der Wirtschaftskriminalität. Wenn ich das fortsetze: Früher ist man hin zu einer Firma, hat durchsucht, hat umzugskartonweise die Buchhaltung mitgenommen und hat die Leitzordner dann anschließend auf der Dienststelle ausgewertet. Da wäre keiner auf die Idee gekommen, die Fotoalben vom Chef mitzunehmen und die auch anzuschauen. Wenn wir heute aber die IT-Systeme mitnehmen, dann schauen wir alles an, auch die Fotos, die da drauf sind. Und da gibt es keine Begrenzung, weil da ist möglicherweise etwas drauf, was relevant sein könnte, vielleicht ist da auch eine Straftat drauf, die man noch nicht erkannt hat und dann würde man im Zweifelsfall eine nicht erkannte Straftat nicht sanktionieren – da müssen wir Lösungen finden, wie wir zukünftig mit so etwas umgehen. Wenn wir die Auswertung nicht beschränken, wird sie uns erschlagen!

Auch im Bereich der Telekommunikationsüberwachung mit Metadaten. Mir sagen die Kollegen vom FBI, wenn sie beispielsweise gegen eine russischstämmige Gruppierung, organisierte Kriminalität, ermitteln, dann sprechen die Leute, die für die Telekommunikationsüberwachung zuständig sind, zuerst mit den Ermittlern darüber, was die brauchen. Und wenn die die Pizzabestellung beim Italiener nicht brauchen, dann wird

die zwar aufgezeichnet aber nicht ausgeleitet. Und ein Netflix-Film genauso wenig. Und wenn dann später vielleicht einmal der Italiener doch von Relevanz sein würde, dann kann man ja die aufgezeichneten Daten später noch ausleiten. Aber wir müssen aufpassen, dass die Leute draußen vor Ort nicht den Wald vor lauter Bäumen nicht mehr sehen. Und dass wir die Ermittler draußen nicht überlasten. Viele Daten sind ein Vorteil für die Polizei, können aber auch zum Fallstrick werden, wenn die Belegschaft damit überfordert wird. Und das geht nicht ohne die Staatsanwaltschaft, so etwas muss mit denen stets abgestimmt werden.

Letztlich noch das Thema Messenger: Es ist interessant, wie das Thema Messenger auch hier die Diskussion dominiert. Das zeigt ja, wie wichtig die Kommunikation untereinander ist und wie wichtig es auch ist, sich in der Polizei gegenseitig abzustimmen. Im Übrigen aber nicht nur dienstlich. Wir haben ja schon das Problem, dass wir dienstlich keinen gemeinsamen Messenger hinbekommen. Aber wir sollten uns hier nicht der Illusion hingeben, dass die Einsatzgruppen, die Dienstgruppen auch privat miteinander kommunizieren müssen: Da fällt jemand aus, wird jemand krank, wer kann morgen für denjenigen einspringen? Es gibt einen Sondereinsatz und mit dem hat man nicht geplant. Da muss man die Kollegen, die in der Freischicht sind, im Zweifelsfall alle, erreichen, dass die auf die Dienststelle kommen. Es gibt Bundesländer, die haben sowas eingeführt, die haben auf dem privaten Handy so eine Applikation, die lässt sich, auch, wenn das Handy auf dem Tisch liegt, nicht vom Ehepartner oder jemand anderem öffnen, weil es noch einmal separat gesichert ist und da kann man so eine Kommunikation ablaufen lassen. Aber das sind die wenigsten, die das haben. Also wir kommen über das dienstliche Kommunizieren über Messenger noch weit hinaus, weil wir akzeptieren müssen, dass auch unter den Kollegen auf den Privathandys in der Freizeit dienstlich notwendige Sachverhalte oder Alarmierungen zu erfolgen haben. Danke.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir nun zu Herrn Gadorosi.

SV **Holger Gadorosi** (Bundeskriminalamt, Wiesbaden): Vielen Dank.

Ich nutze gerade die Messenger-Vorlage, um auf die Frage nach dem Anpassen von Begrifflichkeiten einzugehen. Ich weiß gar nicht, ich glaube, jeder im Raum hat heute schon „Messenger“ im Mund geführt. Wenn Sie draußen einen Polizisten fragen: „Was ist ein Messenger?“, kriegen Sie zig verschiedene Antworten. Herr Schneider hat schon die Spezialeinsatzkräfte erwähnt, für die haben wir nahezu bundesweit eine gemeinsame Lösung. Wenn die zusammen im Einsatz sind, haben wir eine gemeinsame Messenger-Lösung. Die denken natürlich, wenn man von „Messenger“ spricht, an ihre Lösung. Der normale Schutzpolizist denkt an etwas ganz anderes. Der braucht nicht die SEK-Lösung, die ist für den viel zu umfangreich, der will auf die Schnelle kommunizieren. Der Nächste denkt bei einer Messenger-Lösung gar nicht polizeiintern, sondern der muss mit den Rettungskräften, mit der Feuerwehr kommunizieren. Also wir müssen die Messenger-Lösung sicherlich auch größer denken – eine reine Polizei-Lösung hilft, aber die ist auch noch nicht das Ende. Von daher: Allein in dem Begriff „Messenger“, der für uns alle irgendwie vorbelegt ist, sieht man, dass wir in der heterogenen Polizeiwelt dann von ganz unterschiedlichen Begrifflichkeiten reden.

Und wenn man jetzt noch berücksichtigt, dass wir derzeit bei den Kernsystemen von mehr als 6.000 Einzelinformationen sprechen, die einen Polizeialltag ausmachen – über 6.000 unterschiedliche Informationen: von einem Führerschein angefangen, über eine Personalie, Fingerabdrücke und so weiter und so fort, was sich da alles dahinter verbirgt – haben wir in unserem Datenmodell, unserem Informationsmodell, derzeit schon mehr als 6.000 Informationen, die zum Teil unterschiedlich interpretiert werden. Wenn man die vereinheitlichen und harmonisieren möchte, müssen sie natürlich auch von der Begrifflichkeit und von der

Anwendung und von der Interpretation harmonisiert werden. Es reicht nicht nur, die technisch hinzustellen, sondern es muss auch jeder das Gleiche dahinter verstehen und das Gleiche daraus interpretieren, damit die Ergebnisse oder die Daten, die er einfügt, der andere Kollege auch richtig interpretiert und auswertet, wenn der die Daten liest. Nur einmal ein Beispiel: Eine Demonstration oder eine Versammlung, je nachdem, vielleicht wähle ich den Begriff „Demonstration“ ganz bewusst und nicht „Versammlung“. Der Kollegen interpretiert es aber vielleicht als Synonym. Auch solche Dinge müssen vereinheitlicht werden. Und das ist ein langwieriger Prozess und muss letztendlich jede Kollegin und jeden Kollegen erreichen.

Zum Thema Statistiken: Das Ziel, das wir mit Polizei 2020 verfolgen, ist dieses gemeinsame Datenhaus. Das heißt, ein Datum wird erfasst und wird direkt in diesem gemeinsamen Datenhaus gespeichert und verwaltet und dort dann entsprechend weiter qualifiziert. Das wird nicht mehr transportiert, sondern kommt ins Datenhaus, bleibt im Datenhaus, wird dort qualifiziert, wird dort auch wieder gelöscht, wenn es zu löschen ist. Das muss das System sicherstellen. Da die Daten von Anfang an im Datenhaus sind, haben wir natürlich ganz andere Möglichkeiten, ein Frühwarnsystem aufzusetzen, um vor die Lage zu kommen, Trends zu erkennen. Weil die Daten nicht mehr in irgendeiner Dienststelle schlummern und irgendwann, wenn sie keinen mehr interessieren, weil sie bis zum letzten Informationsgewinn ausgelutscht sind, erst weitergegeben werden – was in der Regel viel zu spät ist – sondern von Beginn an in dem Datenhaus sind und auf einer sicheren Rechtsgrundlage verarbeitet und interpretiert und auch extrapoliert und in die Zukunft gedacht werden können.

Genauso natürlich für die Analysefähigkeit von Herrn Dr. Egbert: Da haben wir ja einen Screenshot von dieser Palantir-Software in der schriftlichen Ausarbeitung drin. Die Software zeichnet sich unter anderem dadurch aus, dass sie die verschiedensten Datenquellen zusammenzieht und die Daten analysierbar macht. Das brauchen wir so nicht mehr, wenn wir unser gemeinsames Datenhaus haben. Dann sind die Polizeidaten in dem Datenhaus und wir müssen nicht mehr unterschiedlichste Daten irgendwo her –ich will gar nicht wissen, woher die dann immer kommen – zusammenziehen, sondern die für die Polizeiarbeit relevanten Daten, die sind im Datenhaus und können dort dann auch transparent auf einer gesicherten – auch datenschutzrechtlich – Basis ausgewertet und nachvollziehbar weiterverarbeitet werden. Ein riesen Schritt also. Nicht nur für die operative Arbeit, sondern auch für das ganze Thema Frühwarnungen, Analysefähigkeit, dieses gemeinsame Datenhaus. Danke schön.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann kommen wir nun zu Herrn Dr. Egbert.

SV **Dr. Simon Egbert** (Universität Bielefeld): Vielen Dank.

Da kann ich direkt anschließen. Herr Gadorosi hat ja jetzt das Palantir-Programm erwähnt und den Screenshot und darauf zielte ja auch die Frage ab zu Überwachungsdynamiken und Überwachungserweiterung und wie man dem Herr werden kann. Und in der Tat reicht es nicht aus zu sagen, dass wir uns jetzt nur rein auf Polizeidaten fokussieren. Das ist natürlich durchaus ein Fortschritt, wenn man eben nicht auch noch wild Daten von externen Datenanalyse-Firmen beziehungsweise Data Providers hinzukauft. Allerdings sollten auch die polizeilich bereits vorliegenden Daten reduziert werden für diese Systeme. Und das, denke ich, ist ganz wichtig, dass, wenn Personenbezug notwendig ist, dann bitte schön nur für solche Personen, die auch wirklich als Täter*innen in Frage kommen und nicht auch Datenerhebung zur Analyse bereitstellen für Personen, die erst einmal gar nichts damit zu tun haben, sondern dann durch die Analysesoftware erst einmal ja, dass da irgendwie ein Zusammenhang erstellt wird. Und das ist ja der Punkt, der relativ abstrakt sein kann, wie in diesem Screenshot dargestellt, dass es einfach erst

einmal darum geht, dass die Personen in irgendeiner Weise in Kontakt standen. Das hat den/die Polizist*in, die den Fall gerade bearbeitet, erst einmal nicht zu interessieren. Und diese Zugriffe auf personenbezogene Daten sollten erst möglich sein, wenn sich wirklich andeutet, dass wir hier eine weitere Person haben, die mit der Tat in irgendeiner Weise in Zusammenhang steht und damit etwas zu tun hat. Und diese Hinweise sollten eben nicht allein oder von vornherein über eine Software kommen, sondern sich auch aus anderen Ermittlungssträngen herleiten lassen.

Wichtig ist aber auch, dass wir hier eben nicht nur über technische Vorkehrungen sprechen sollten, sondern eben auch wieder über Schulungen und Ausbildung – sprich: Die Kompetenz der Anwender*innen, mit diesem System dann datenschutzkonform umzugehen, muss durch Schulung und Ausbildung entsprechend ermöglicht werden. Ein Beispiel ist eben das raumbezogene predictive policing, wo es darum geht, dass eine Prognosesoftware das Risiko in bestimmten Räumen vorhersagt, dass da Kriminalität – in den meisten Fällen geht es um Wohnungseinbruchdiebstahl – dass das da passiert und wenn die Kolleginnen und Kollegen dann einen „ökologischen Fehlschluss“ begehen und in dem Risikoort sind und dann das Risiko des Ortes auf die dort vorhandenen Personen projizieren und die dann gleichsam offensiver kontrollieren, dann ist dem insgesamt eben auch nicht damit gedient, dass diese personenbezogenen Daten in dem System nicht vorgesehen sind oder nicht eingespeist werden. Das heißt, der kompetente Umgang muss auch hier garantiert sein durch eine adäquate Schulung. Nur so kann dieses secondary surveillance network, was Sarah Brayne anspricht, diese Ausweitung des Überwachungsblickes, nur so kann der verhindert werden.

Ich möchte auch noch kurz eine Teilfrage aus der ersten Runde beantworten, wo es darum ging, wie verhindert werden kann, dass Daten aus der Polizei rauskommen. Ich denke, dass da bei Hessendata – also der Palantir-Software, die in Hessen angewendet wird – tatsächlich schon gute erste Ansätze bestehen. Das bedeutet konkret, dass Palantir-Mitarbeiter*innen in die Polizeibehörde kommen müssen, um dort an speziell hergerichteten Computern, die eben nicht ins Polizeinetzwerk – komplett zumindest – Zugriff haben, dass die dort vor Ort mit den Daten arbeiten und die Palantir-Software – das ist ja der Marken-Claim – speziell für die Polizei administrieren und herrichten. Und diese Arbeiten müssen zwingend vor Ort durchgeführt werden, weil alles andere bedeutet, dass entsprechende Daten rausgehen müssen, sei es jetzt nach Palo Alto oder auch nach München, wo ja Palantir auch einen Sitz hat. Also das muss definitiv sichergestellt werden, damit Daten eben nicht rausgehen und für Externe einsehbar sind. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Wir kommen zu den Antworten von Herrn Professor Aden.

SV **Prof. Dr. Hartmut Aden** (Hochschule für Wirtschaft und Recht, Berlin): Vielen Dank.

Die Diskussion über die Messenger-Dienste hat gezeigt, dass es dort noch sehr viel Handlungsbedarf gibt. Ich habe jetzt hier noch keine wirklich überzeugende Lösung gehört. Der Ausgangspunkt ist ja erst einmal, dass junge Menschen heute über WhatsApp kommunizieren. Das merke ich, wenn ich Studierende im ersten Semester habe und die sich untereinander vernetzen wollen. Wir haben natürlich auch wunderschöne Hochschulsysteme, die sie nutzen könnten. Dann müssten sie sich erst einmal einloggen, aber dann könnte ich als der Prof‘ auch mitlesen, und ich verstehe auch, dass sie einmal auch ohne mich kommunizieren wollen, alles wunderschön. Die nutzen also WhatsApp, auch die Polizeistudierenden. Aber dann kommen sie in die Praxis und stellen fest, oh, die Behörde hat so etwas ja gar nicht und was machen sie? Sie nutzen dann für die dienstliche Kommunikation auch WhatsApp. Das geht natürlich überhaupt nicht.

Und es geht auch insofern nicht – das haben wir auch gerade in verschiedenen Bundesländern in den letzten Monaten erlebt: Was machen da einige eigentlich in diesen WhatsApp-Gruppen? Strafbare Inhalte austauschen, extremistische Tendenzen pflegen und ähnliches. Das ist eine Entwicklung, die wir meines Erachtens wirklich sehr sorgfältig im Blick behalten müssen. Was wäre die Lösung? Ich denke, wir bräuchten tatsächlich ganz am Anfang, wenn jemand bei der Polizei anfängt, eine Messenger-Software, die für alle zur Verfügung steht. Dann istklar:‚Das ist mein privater Bereich – mit meiner Großmutter kann ich gern über Whats-App in Kontakt sein, aber sobald es dienstlich ist mit den Kolleginnen und Kollegen, muss es auf ein dienstliches System gehen. Das löst allein noch nicht alle Probleme, die es gibt, was etwa sensible Daten angeht. Was aus meiner Sicht ein absolutes No Go, aber doch gängige Praxis ist – man hat eben kein Messenger-System, muss aber dringend ein Foto vom Tatort von Verletzten odervon Tatverdächtigen an die Dienststelle geben - da wird das mal eben mit WhatsApp gemacht. Da kriegt man als jemand, der da etwas sensibilisiert ist, einen großen Schreck. Aber ich kann Ihnen versichern, das habe ich mehr als einmal irgendwo gehört. Das heiß, da brauchen wir auch sehr viel Sensibilisierung dafür, dass das absolut nicht geht.

Wenn es aber geht, weil wir ein eigenes System haben, dann brauchen wir, glaube ich, sehr viele technische und organisatorische Vorkehrungen, damit dieses zusätzliche Messenger-System nicht plötzlich genutzt wird, um die ganzen Berechtigungskonzepte, die ja in dem Polizei 2020-Papier so schön drinstehen, zu umgehen, weil man dann die Daten einmal so eben da hinüberzieht und dann mit seiner großen Gruppe dort teilt. Da liegen wirklich ganz große Herausforderungen, wo ich denke, da sind heute auch noch einmal die Handlungsbedarfe deutlich geworden, aber auch, dass wir da leider erst ganz am Anfang stehen. Da muss wirklich sehr stark mit Design-Elementen gearbeitet werden.

Ich bin auch nicht der Meinung, dass die Polizei eigene Smartphones entwickeln sollte, das würde, glaube ich, überhaupt nicht funktionieren. Aber ich denke, bei diesen Software-Lösungen werden wir nicht darum herum kommen. Da können wir nicht mit den Standardanbietern arbeiten, weil wir sonst die gleichen Probleme haben werden, wie bei der KI-Software, dass am Ende die Daten irgendwo liegen und auch kein Mensch so ganz genau weiß, was eigentlich damit passiert. Das heißt, das muss definitiv für die polizeiliche Kommunikation ein eigenes System werden – von mir aus gern ein bundeseinheitliches, damit dann diese ganzen Unterstützungseinsatzsituationen auch gleich mitgelöst sind. Aber dann muss auch die Frage geklärt sein, wie viel Einfluss die Behörde darauf nehmen muss, wer was mit wem kommuniziert. Und da denke ich, sind wir doch auch wieder beim Faktor Mensch. Wir können da vieles durch Design abfedern, aber am Ende brauchen wir da auch sehr viel Aus- und Fortbildung, damit klar ist: Bestimmte Dinge gehen damit schlicht und ergreifend nicht. Und man muss tatsächlich auch in der Lage sein, im Polizeidienst Privat- und Berufsleben zu trennen, und da auch eine Sensibilität entwickeln. Da haben wir, die in der Aus- und Fortbildung tätig sind, sicherlich große Baustellen vor uns.

Wen könnten wir als internationale Vorbilder nehmen? Ich finde immer noch spannend, auf die kleinen Länder zu schauen, die nach 1990 alles neu machen mussten. Ich war vor einigen Jahren mit meinen Studierenden bei der Polizei in Estland. Die Esten waren sicherlich führend und haben allerdings das „Glück“ gehabt, dass es erstens ein kleines Land ist und zweitens, dass sie aufgrund von Korruption die komplette ältere Generation bei der Polizei nach Hause geschickt haben. Insofern hatten sie eine gute Ausgangsposition, um technische Innovationen einzuführen. Da ist sicherlich manches dabei, was inzwischen in Deutschland auch so langsam ankommt. In Estland gab es vor zehn Jahren eigentlich schon auf jedem Streifenwagen ein mobiles IT-Gerät – das ist da schon sehr

lange Standard. Die sind inzwischen schon bei der zweiten oder dritten Generation. Das sind alles gute Sachen, aber auch, was die Design-Elemente gegenüber den Betroffenen angeht, gibt es da einige interessante Sachen, über die man hier einmal weiter nachdenken könnte: Etwa, dass es in Estland ein Bürgerinnen- und Bürgerportal gibt, über das Menschen abrufen können, was eigentlich der Staat über sie weiß. Das ist ja ein ganz zentrales Transparenz-Element – davon sind wir noch extrem weit entfernt. Und warum nicht das auch für bestimmte Themen im Polizeibereich mit nutzen? Also etwa war vorhin ja auch die Frage aufgekommen, muss man nicht in diesem Datawarehouse sehr viel stärker differenzieren, was ist mit den Daten der Zeugen und Hinweisgeber? Die kann man da ja nicht genauso behandeln, wie die Daten der Tatverdächtigen. Und sollte dann nicht eigentlich ein System so designt sein, dass die Zeugen und Hinweisgeber auch im Rahmen einer solchen Bürgerabfrage den Hinweis bekommen, ich bin da beim BKA im Warehouse und kann da nachfragen, wie das kommt und ob das nicht eigentlich schon längst hätte gelöscht werden müssen. Das ersetzt aber natürlich nicht das eigene Datenqualitätsmanagement, weil wir ja nicht davon ausgehen können, dass am Ende alle Menschen von morgens bis abends in diese Portale hineinschauen. Das heißt, trotzdem muss im Rahmen des Datenmanagements auch sehr viel gemacht werden, damit die Daten wirklich aktuell und akkurat sind, damit wirklich Löschkonzepte umgesetzt werden. Das sind alles Dinge, wo noch sehr viel im Argen liegt. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Danke schön. Dann bedanke ich mich bei allen Sachverständigen. Wir sind am Ende der Anhörung angekommen und haben eine exakte Punktlandung. Ich schließe die Sitzung um 11:30 Uhr. Danke.

Schluss der Sitzung: 11:30 Uhr

Jochen Haug, MdB
Stellv. Vorsitzender

Dr. Simon Egbert
simon.egbert@uni-bielefeld.de

04.06.2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Ausschussdrucksache
19(4)863 A

Stellungnahme zum Antrag der FDP-Fraktion ‚Smart Police – Digitalisierung der deutschen Polizei anschieben' – Drucksache 19/27172 (02.03.2021)

Die Digitalisierung bietet selbstverständlich auch für die Polizei erhebliches Potenzial in Hinblick auf die Verbesserung ihrer Arbeit. Allerding sollte man nicht dem Trugschluss verfallen, dass digitale Technologien per se und gleichsam automatisch eine effektivere und/oder effizientere Polizeiarbeit ermöglichen. Vielmehr ist die erfolgreiche Implementierung von digitalen Technologien – nicht nur, aber vor allem bei der Polizei – überaus voraussetzungsvoll (vgl. Egbert/Leese 2021). Gleichzeitig ist die Einführung von digitalen Technologien stets mit Risiken verbunden, die im Rahmen jeglicher Pilotierungs- wie Implementierungsbemühungen reflektiert und konsequent in Rechnung gestellt werden müssen (vgl. Ferguson 2017).

Diesbezüglich gilt es zunächst auf ein grundsätzliches Faktum hinzuweisen: Digitalisierte Praktiken sind stets soziotechnische Praktiken, digitale Technologien immer und unumgänglich auch soziale Technologien. Dies impliziert u. a., dass algorithmische Analysen keineswegs per se neutrale oder objektive Ergebnisse liefern. Zu glauben, digitale Technologien könnten von sich aus für eine neutrale Risikobewertung sorgen, ist ohnehin naiv. Bei der Programmierung von Algorithmen und der Auswahl der zu analysierenden Daten sind vielfältige menschliche Entscheidungen zu treffen, die allesamt das Potenzial von Verzerrungen bergen (z. B. boyd/Crawford 2012: 666ff.; Kitchin 2017: 14f.).

Es stimmt selbstredend, dass ein Algorithmus stets strikt gemäß seiner Programmierung entscheidet und sich dabei nicht von Gefühlen, Vorteilen o.ä. leiten lässt – diese Entscheidungen kann er aber nur auf Basis einer Weltsicht treffen, die die ihm vorliegenden Daten ermöglichen. Liegen einer algorithmischen Analyse verzerrte Daten zu Grunde, kann kein neutrales Ergebnisse mehr am Ende der Analyse stehen (vgl. Abb. 1). Dieser Punkt ist bei Analysetechnologien, die mit polizeilichen Daten arbeiten, hochrelevant, ist doch seit Jahren, in nationalen wie internationalen Studien ebenso breit wie überzeugend belegt, bekannt, dass die Wahrscheinlichkeit für ethnische Minderheiten, in den Fokus der Polizei zu geraten, überproportional hoch ist (Glover 2009; Glaser 2014; Herrnkind 2014; Behr 2018). Darauf folgt, dass Personen betroffener Gruppen in polizeilichen Datenbanken überrepräsentiert sind, was ein Algorithmus für sich genommen aber nicht als Folge diskriminierender Polizeipraktiken zu erkennen vermag, sondern viel eher als Beleg interpretiert, dass derlei Personen ein höheres Kriminalitätsrisiko aufweisen – was zu diskriminierenden Verstärkerprozessen führen kann, da die

algorithmischen Risikoanalysen den polizeilichen Fokus auf bereits überpolizierte Bevölkerungsgruppen nochmals verstärken (z. B. O'Neil 2016).

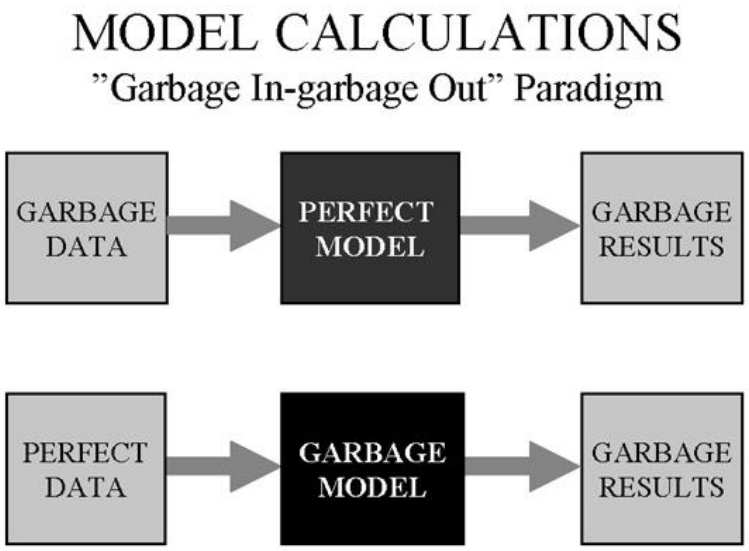

Abbildung 1: *Garbage in, Garbage out-Modell (Quelle: http://left.mn/2014/02/polymet-knew-now-knew/)*

Dieses Problem verschärfend und bereits unter dem Schlagwort „tech-washing" diskutiert, können diese diskriminierenden Verstärkereffekte unbemerkt auftreten, indem sie nämlich von den Technologien selbst erzeugt werden. So kann die autonome Herstellung von Risikokorrelationen in großen Datenmengen durch selbstlernende und (weitestgehend) unüberwachte Algorithmen dazu führen, dass algorithmisch eigenständig diskriminierende Verbindungen, z. B. zwischen Hautfarbe und individuellem Kriminalitätsrisiko, konstruiert werden, wobei die nachträgliche Entdeckung und Eliminierung dieser Fehldeutungen überaus schwierig ist, da entsprechende Algorithmen immer auch als Black Box fungieren und oft – auch für die beteiligten Polizisten und Polizistinnen – uneinsehbar sind (Pasquale 2015).

Dies führt mich zu meinem nächsten Punk: Transparenz.

Die Zusammenarbeit mit Industriepartnern aus der Digitalwirtschaft birgt für die Polizei die grundsätzliche Gefahr, mit Instrumenten und Werkzeugen zu arbeiten, die tief in den organisationalen und praktischen Alltag von Polizistinnen und Polizisten eingreifen, gleichzeitig aber für jene auf Grund ihres proprietären Charakters weitestgehend intransparent bleiben. Dies muss so weit wie möglich verhindert werden, da ein kompetenter und kritischer Umgang mit derartigen Technologien sonst nicht möglich ist. Ein hinreichender Einblick in die Grundannahmen und -prinzipien der genutzten Technologien muss den Anwenderinnen und Anwendern innerhalb der Polizei zwingend gewährleistet sein.

Dies gilt ebenfalls für die Bürgerinnen und Bürger, denen gegenüber die Polizei begründungspflichtig ist. Trotz legitimer Geheimhaltungsinteressen muss auch die Bevölkerung eine hinreichend präzisen Einblick in die Arbeitsweise der polizeilich genutzten digitalen Technologien bekommen können. Dies gilt selbstredend ebenfalls und noch stärker für Richterinnen und Richter sowie für die Rechtsbeistände von angeklagten Personen, wenn in betreffenden Verfahren solcherart Technologien relevant sind. Auch und gerade im Falle digitalisierter Polizeipraktiken muss die Prüfung der Rechtmäßigkeit der erhobenen Vorwürfe umfassend möglich sein (z. B. Singelnstein 2018).

Ferner möchte ich auf die möglichen Folgen der polizeilichen Zusammenarbeit mit Industriepartnern aus der Digitalwirtschaft hinweisen.

Der Rechtstreit zwischen dem New York Police Department und der Firma Palantir (s. z. B. Price/Hockett 2017) hat gezeigt, dass sich Polizeibehörden zumindest potenziell in eine starke Abhängigkeit begeben, wenn sie ihre Erkenntnisse mit Hilfe kommerzieller Software generieren. Denn nachdem die New Yorker Polizei den Vertrag mit Palantir kündigen wollte, hat Palantir darauf bestanden, die mit ihrer Software gewonnenen Erkenntnisse nach Vertragsende dem Zugriff der New Yorker Polizistinnen und Polizisten zu entziehen.

In diesem Zusammenhang gilt es ebenfalls zu fragen, wie stark und übergreifend eine kommerzielle Software in die technische Infrastruktur von Polizeibehörden eindringen sollte, ohne dass etwaige Folgevertragsverhandlungen über Gebühr einseitig verlaufen, wenn nämlich die gesamte polizeiliche Datenhaltungs- und Kommunikationsinfrastruktur auf der betreffenden Software aufbaut und die Folgekosten eines Vertragendes für die Polizei exorbitant hoch wären.

Fakt ist, dass durch die zunehmende Datafizierung der Polizei externe Akteure tief in den operativen Alltag der Polizei vordringen, womit zahlreiche Risiken verbunden sind. Dazu zählt insbesondere, dass gesichert werden muss, dass Unbefugte keinen Zugriff auf sensible polizeiliche Daten haben. Ebenso muss gesichert sein, dass so wenig Daten wie möglich aus den Polizeibehörden herausgeben werden.

Nun zu meinem letzten Punkt: Überwachung.

Internationale Studien haben bereits festgestellt, dass digitalisierte Polizeipraktiken das Potenzial haben, Überwachungspotenziale der Polizei zu vervielfältigen. So schildert Brayne (2021) in Bezug auf die Nutzung von Palantir-Software des Los Angeles Police Department das Phänomen der „dragnet surveillance“ (dt.: Schleppnetz-Überwachung), welches eines substantielle Ausweitung des überwachenden Blickes impliziert, da durch die auf Verbindungsanalysen

(„link analyses“) spezialisierte Palantir-Software auch solcherart Personen in den Fokus der Polizei rücken, die bis dato noch keinen Kontakt zur Polizei hatten – weil sie mit verdächtigen Personen in Kontakt stehen (vgl. Abb. 2). Eine solche Spielart von Kontaktschuld (auch „guilt by association“ genannt) darf keinesfalls Gegenstand polizeilicher Analysetätigkeiten werden.

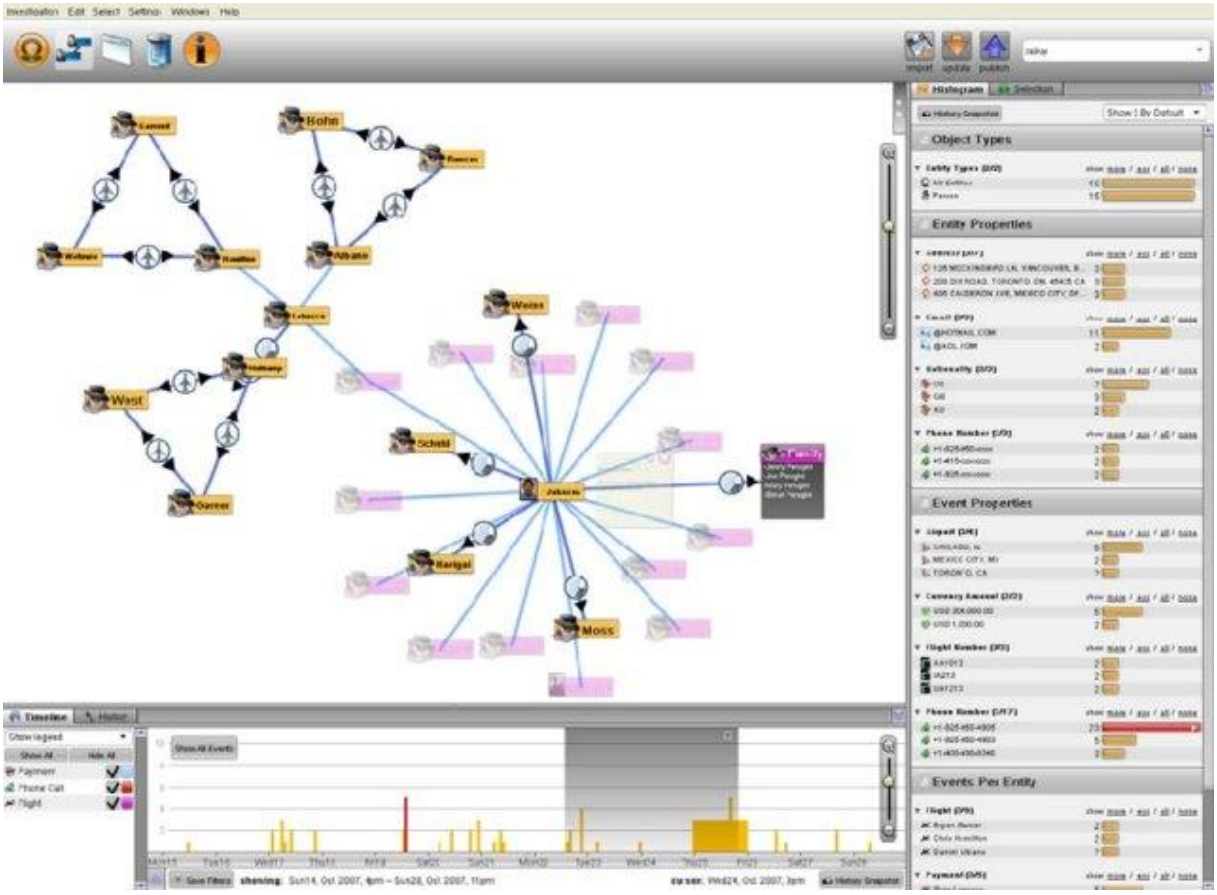

Abbildung 2: *Palantir Gotham-Screenshot (Quelle: https://www.researchgate.net/profile/Brian-Ulicny/publication/230818105/figure/fig2/AS:340539108020226@1458202258875/Palantir-Screenshot-from-Palantir-Tech-Blog-The-graph-is-linked-to-the-histogram-view_W640.jpg)*

Neue Datenanalysealgorithmen in den Händen der Polizei haben ebenso das Potenzial, die Überwachung von bereits polizeibekannten Personen zu intensivieren, indem beispielsweise automatische Alarme aktiviert werden können (z. B. durch sogenanntes „geofencing“, mit dem sich Areale vordefinieren lassen, bei dessen Betreten von ausgewählten Personen automatisch eine Alarmmeldung ausgelöst wird).

Und nicht zuletzt bergen avancierte Datenanalysealgorithmen die Gefahr, einen starken institutionellen Anreiz pro Datensammlung zu erzeugen, da sie umso besser funktionieren, je zahlreicher und heterogener die Daten sind, auf die sie zugreifen können. Datenanalyseplattformen wie Palantirs Gotham können ihr volles analytisches Potential beispielsweise nur dann

ausschöpfen, wenn sie auf viele verschiedenen Datentöpfe gleichzeitig zugreifen können (vgl. Egbert 2020).

Entsprechenden Dynamiken muss früh genug Einhalt geboten werden, um weitreichende Rechtsverletzungen zu unterbinden.

Literatur

Behr, Rafael (2018) Rassismus und Diskriminierung im Polizeidienst. *SIAK-Journal* 13: 57-66.

boyd, danah; Crawford, Kate (2012): Critical Questions for Big Data. *Information, Communication & Society* 15(5): 662-679.

Brayne, Sarah (2021): *Predict and Surveil. Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

Egbert, Simon (2020): Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen. In: Hunold, Daniela; Ruch, Andreas (Hrsg.): *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts*. Wiesbaden: Springer VS, S. 77-100.

Egbert, Simon; Leese, Matthias (2021): *Criminal Futures. Predictive Policing and Everyday Police Work*. London/New York: Routledge.

Ferguson, Andrew Guthrie (2017): *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Glaser, Jack (2014): *Suspect Race. Causes and Consequences of Racial Profiling*. Oxford: Oxford University Press.

Glover, Karen S. (2009): *Racial Profiling. Research, Racism, Resistance*. Lanham et al.: Rowman & Littlefield.

Herrnkind, Martin (2014) „Filzen Sie die üblichen Verdächtigen!“ oder: Racial Profiling in Deutschland. *Polizei & Wissenschaft* 15 (3): 35-58.

Kitchin, Rob (2017): Thinking critically about and researching algorithms. *Information, Communication & Society* 20(1): 14-29.

O’Neil, Cathy (2016): *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. London: Penguin Books.

Pasquale, Frank (2015): *The Black Box Society. The Secret Algorithms that Control Money and Information*. Cambridge/London: Harvard University Press.

Price, Michael; Hockett, Emily (2017): *Palantir Contract Dispute Exposes NYPD’s Lack of Transparency*, 20. Juli 2017. https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency [abgerufen am 04.06.2021].

Singelnstein, Tobias (2018): Predictive Policing. Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. *Neue Zeitschrift für Strafrecht* 1/2018: 1-9.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)863 B

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Prof. Dr. Hartmut Aden
Fachbereich 5
Polizei und Sicherheitsmanagement
Professur für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft

Mitglied des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS Berlin)

Alt-Friedrichsfelde 60
D-10315 Berlin
T +49 (0)30 30877-2868

privat:
Postfach 580601
D-10415 Berlin

E-Mail: Hartmut.Aden@hwr-berlin.de

www.hwr-berlin.de/prof/hartmut-aden

www.foeps-berlin.org

Prof. Dr. Aden, HWR Berlin • Alt-Friedrichsfelde 60 • 10315 Berlin

An den
Ausschuss für „Inneres und Heimat“ des
Deutschen Bundestages

Per E-Mail an: innenausschuss@bundestag.de

Datum: 05. Juni 2021

Stellungnahme zum Antrag
„Smart Police – Digitalisierung der deutschen Polizei anschieben“, Bundestags-Drs. 19/27172 vom 2. März 2021,
vorgelegt zur Anhörung des Ausschusses für „Inneres und Heimat“ des Deutschen Bundestages am 7. Juni 2021 in Berlin

Sehr geehrte Damen und Herren,

ich danke Ihnen für die Einladung zur Anhörung. Die Befassung Ihres Ausschusses mit diesem wichtigen Thema ist zu begrüßen. Der vorliegende Antrag enthält einige zutreffende Analysen, ist aber auch durch Auslassungen und eine eingeschränkte Perspektive geprägt; daher sollte sich der Deutsche Bundestag diesen Text nur nach gründlicher Überarbeitung zu eigen machen. Die folgende Stellungnahme kann nicht auf alle Teilthemen des Antrags eingehen. Sie konzentriert sich auf fehlende bzw. unzulänglich gewichtete Aspekte, die der Deutsche Bundestag – teils in Zusammenarbeit mit der Landesgesetzgebung – bei gesetzgeberischen Weichenstellungen für die weitere Digitalisierung der Polizeiarbeit berücksichtigen sollte.

1. Digitalisierung im Kontext polizeilicher Techniknutzung

Die Polizeiarbeit ist nicht erst seit der unter dem Stichwort *Digitalisierung* diskutierten neueren Entwicklungen in hohem Maße von Informationen abhängig. Möglichkeiten, die Informationsbeschaffung und –verarbeitung zu verbessern und zu vereinfachen, sind daher seit vielen Jahrzehnten ein Thema polizeipolitischer Diskussionen.

1.1 Entwicklungsdynamik der polizeilichen Techniknutzung seit den 1970erJahren

Aufgrund langwieriger Beschaffungsprozesse und begrenzter Haushaltsmittel bleibt die Technikausstattung von Verwaltungen – und auch der Polizei – typischerweise weit hinter der Ausstattung privater Unternehmen zurück. Insbesondere an der „Verwaltungsbasis“ kommen Innovationen daher oft nur mit großer zeitlicher Verzögerung an.[1]

Auch und gerade im Polizeibereich ist Digitalisierung indes keine neue Entwicklung, sondern ein fortlaufender Prozess, der sich bereits auf die 1970er Jahre zurückführen lässt, als insbesondere das Bundeskriminalamt weitreichende Ambitionen entwickelte, die Möglichkeiten der sich seinerzeit dynamisch entwickelnden Informationstechnologie zu nutzen.[2] Noch vor wenigen Jahrzehnten mussten etwa Fahndungen und Fingerabdrücke manuell auf Karteikarten erfasst und abgeglichen werden. Im Vergleich zu jener Phase hat auch die Polizeiarbeit bereits sehr große Technisierungs- und insbesondere Digitalisierungssprünge gemacht. Nach den Terroranschlägen in den USA vom 11. September 2001 wurden in der EU und in Deutschland zudem umfangreiche Forschungsprogramme aufgelegt, in denen die Weiterentwicklung von Sicherheitstechnik eine zentrale, bisweilen sogar (zu) dominante Stellung eingenommen hat.

Die föderale Struktur der deutschen Polizei führt – wie im Antrag zutreffend dargelegt – dazu, dass Potenziale für Synergien bei der Technikentwicklung und -nutzung nicht immer optimal genutzt werden. Allerdings sollte auch nicht übersehen werden, dass die föderale Struktur das deutsche Polizeisystem bei Innovationen flexibler macht. Regionale Besonderheiten können so besser berücksichtigt werden. Bei der Digitalisierung haben einzelne Landespolizeien die Möglichkeit, mit Innovationen voranzugehen, die im Falle der praktischen Bewährung von anderen übernommen werden können.

1.2 Digitalisierung von Arbeitsabläufen und von Datenverarbeitungsvorgängen: Grundrechtliche Dimensionen einbeziehen

Der vorliegende Antrag vernachlässigt die grundrechtlichen Dimensionen der Digitalisierung im Polizeibereich. Für die erforderlichen gesetzgeberischen Weichenstellungen empfehle ich die Unterscheidung zwischen der

---

1 Näher zu diesem Strukturproblem Aden 2019.

2 Vgl. etwa Herold 1979; zur kritischen Bewertung Nogala 1989; zur weiteren Entwicklung: Zachert 1991.

Digitalisierung von Arbeitsabläufen ohne zusätzliche Grundrechtseingriffe gegenüber Dritten und solchen Digitalisierungsschritten, die sich auf die Erhebung und weitere Verarbeitung personenbezogener Daten beziehen.

Die im Antrag erwähnte softwareunterstützte Transkription von Vernehmungsprotokollen könnte als Beispiel für die Digitalisierung von Arbeitsabläufen ohne zusätzliche Grundrechtseingriffe eingestuft werden, auch wenn die Inhalte sich auf – sehr sensible – Daten beziehen. Denn die Vernehmungsdaten sind ohnehin vorhanden und werden auch bisher elektronisch erfasst. Der Weg dahin würde durch eine Softwareunterstützung erleichtert.

Dagegen sind alle Formen von Interoperabilität polizeilicher Datenbanken mit einer erhöhten Eingriffsintensität verbunden, da sie – auch bei restriktiv gestalteten Zugriffsberechtigungen – stets dazu führen, dass mehr Polizeibedienstete auf die Daten Zugriff haben.[3] Der praktische Nutzen von Interoperabilität darf nicht den Blick darauf versperren, dass etwa fehlerhafte Einträge in Datenbanken im Zuge der Interoperabilität polizeilicher Datenbestände zu stark erhöhten Risiken führen – etwa steigt das Risiko rechtswidriger Maßnahmen bis hin zur Festnahme aufgrund von falschen Suchtreffern. Interoperabilitäts-Anforderungen müssen daher stets mit konkreten gesetzgeberischen Vorgaben für die Sicherung aktueller und zutreffender Datenbestände verknüpft werden.

2. Chancen und Risiken der Digitalisierung einbeziehen

Die Gesetzgebung und andere politische Weichenstellungen zur Digitalisierung der Polizeiarbeit sollten Chancen und Risiken in den Blick nehmen und frühzeitig Vorkehrungen treffen, um mit Risiken angemessen umzugehen.

2.1 Akzeptanz der Betroffenen durch Transparenz fördern

Die Diskussion über polizeiliche Digitalisierungsbedarfe nimmt oft einseitig die Arbeitseffizienz der Polizeiarbeit in den Blick. Zahlreiche Untersuchungen haben indes ergeben, dass Polizeiarbeit nur dann erfolgreich sein kann, wenn die Betroffenen, in deren Grundrechte eingegriffen wird, die Ziele und Vorgehensweisen der Polizei verstehen und als fair empfinden. Dieser in den USA entwickelte Ansatz (*Procedural Justice Theory*[4]) lässt

---

3 Näher hierzu: Aden 2020a; zur Kritik auch EDPS 2018.
4 Vgl. z. B. Tyler 2017.

sich auch auf den europäischen und deutschen Kontext sowie auf die Digitalisierung der Polizeiarbeit übertragen.

Ein Kernelement der Fairness ist die Nachvollziehbarkeit des polizeilichen Handelns für die Betroffenen – andernfalls besteht ein hohes Risiko, dass sie das Vorgehen als willkürlich empfinden. Die Transparenz polizeilichen Handelns ist nicht nur nach der EU-Datenschutzgrundverordnung geboten, sondern auch für die Teile der strafverfolgenden Polizeitätigkeit, die unter die Richtlinie (EU) 2016/680 fallen, also unter die sogenannte Justiz- und Innen-(JI)-Richtlinie für den Datenschutz im Polizei- und Strafjustizbereich. Da Polizeibehörden daran gewöhnt sind, ihre Arbeit aus (teils nachvollziehbaren) taktischen Gründen gegenüber den Betroffenen intransparent zu lassen, tun sie sich mit Transparenz auch dort schwer, wo Geheimhaltung ganz unnötig ist. Weitgehend ungeregelt und damit intransparent ist etwa die Datenverarbeitung in polizeilichen Vorgangsbearbeitungssystemen, in denen Polizist*innen ihre tägliche Arbeit dokumentieren. Die gesetzlichen Eingriffsbefugnisse knüpfen hier an sehr vage Voraussetzungen an; in der Regel reicht die Erforderlichkeit der Datenverarbeitung für die polizeiliche Aufgabenerfüllung für die Verarbeitung personenbezogener Daten. Empirische Forschungserkenntnisse und konkrete rechtliche Standards zur Nutzung dieser Systeme fehlen.[5]

Im Forschungsprojekt MEDIAN[6] haben wir in Zusammenarbeit mit der Bundesdruckerei eine technische Lösung für verbesserte Transparenz bei polizeilichen Kontrollen konzipiert, die Betroffenen automatisiert eine „Quittung“ bereitstellt. Diese technische Lösung lässt sich in dienstliche Smartphones oder andere Geräte integrieren, die bei Kontrollen verwendet werden. Dort verbleiben aber keine zusätzlichen Daten (siehe auch Abbildung 1).

Die bei einer Personenkontrolle erhobenen Daten werden von der konzipierten Anwendung zusammen mit Angaben zu Zeit, Ort und Grund der

---

5 Näher hierzu Fährmann, Aden & Bosch 2020; Aden 2020b.

6 Das Forschungsprojekt MEDIAN (Mobile berührungslose Identitätsprüfung im Anwendungsfeld Migration, 2018-2021/22, gefördert vom Bundesministerium für Bildung und Forschung, BMBF), erforscht unter Konsortialführerschaft der Bundesdruckerei mobile Technologien, die bei Kontrollen zum Einsatz kommen könnten. Das vom FÖPS Berlin durchgeführte rechtlich-sozialwissenschaftliche Teilprojekt hat u.a. untersucht, ob Kontrollquittungen und -statistiken mit Hilfe mobiler Geräte generiert werden könnten und unter welchen rechtlichen Rahmenbedingungen dies möglich wäre.

Kontrolle an ein Hintergrundsystem gesendet. Mit Abschluss des Vorgangs wird diesen Daten eine Quittungsnummer zugeordnet. Diese enthält einen öffentlichen Schlüssel zur Verschlüsselung der Quittungsdaten, die sich auf einem Server außerhalb der Polizei befinden, z. B. bei den unabhängigen Polizeibeauftragten, die inzwischen von einer Reihe von Bundesländern etabliert wurden. Die Daten werden im nächsten Schritt mit dem öffentlichen Schlüssel, welcher der Quittungsnummer zugeordnet ist, verschlüsselt an den externen Quittungsserver versendet und anschließend zusammen mit dem öffentlichen Schlüssel im Hintergrundsystem gelöscht. Daten über die Kontrolle verbleiben nur auf dem Server der Polizei, wenn ein polizeilicher Vorgang angelegt wird und die polizeiliche Datenverarbeitung in diesem Rahmen rechtmäßig ist. Die verschlüsselten Daten, welche auf dem Quittungs-Server gespeichert sind, können nur durch die Besitzer*innen des privaten Schlüssels ausgelesen werden, also durch die kontrollierten Personen.

Die Polizist*innen führen einen analogen Quittungsblock in einem handlichen Format mit; manuelle Einträge sind nicht erforderlich. Alternativ könnte der Code auch von einem handlichen Druckgerät generiert werden, das auch für andere polizeiliche Zwecke verwendet werden könnte. Ein Quick Response (QR)-Code dient zum vereinfachten Abruf der Quittung. Nach dem Scannen des Codes kann die Quittung als passwortgeschützte PDF-Datei im Browser eines Smartphones oder PCs heruntergeladen werden. Mit der Eingabe des privaten Schlüssels wird die PDF-Quittung als Klartext dargestellt. Sie kann nun ausgedruckt oder für weitere Zwecke verwendet werden. Der private Schlüssel bleibt während des gesamten Vorgangs im Besitz der Kontrollierten. Niemand außer dieser Person kann die Quittungsdaten entschlüsseln. Die Identifizierung der Quittung auf dem Quittungsserver durch den Hashwert verhindert die Herausgabe eines Datensatzes im Fall einer falsch eingegebenen Quittungsnummer.

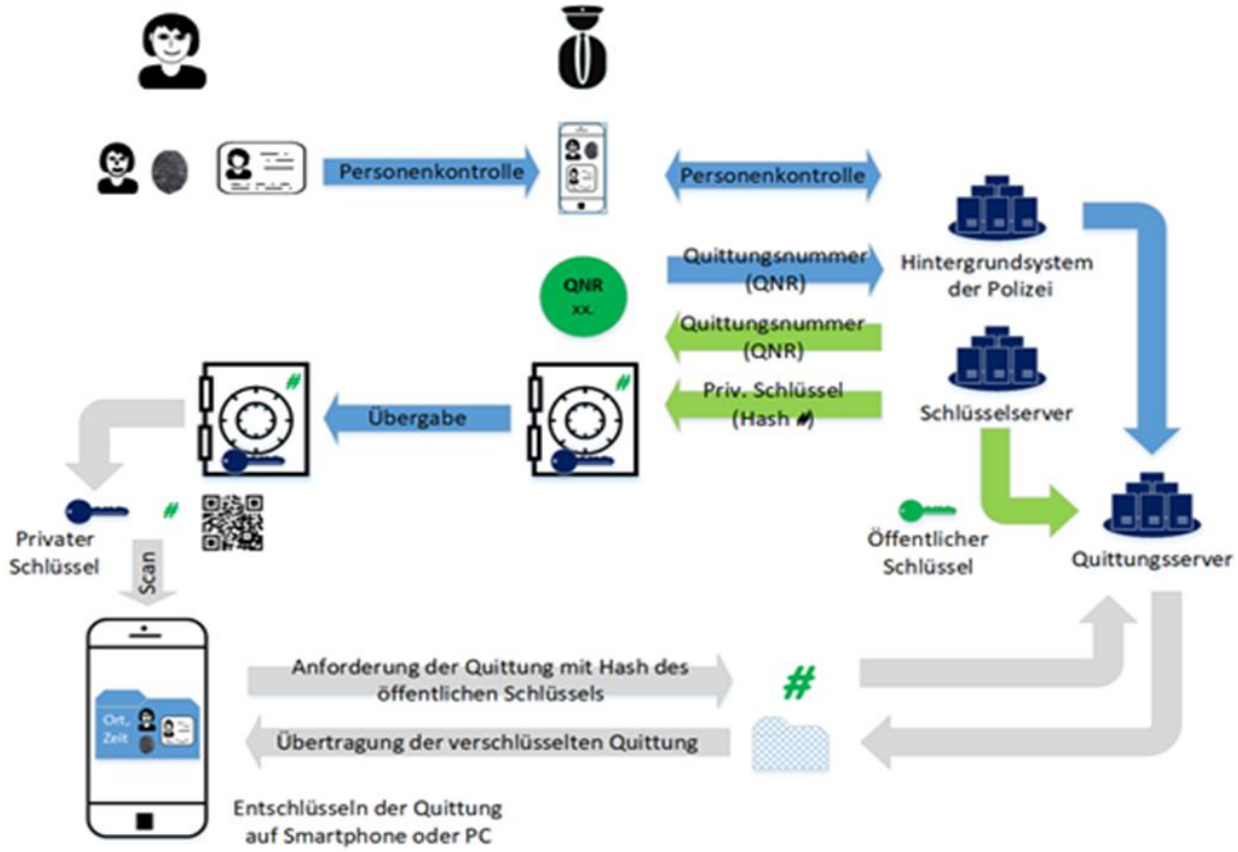

Abbildung 1: Ablauf der Quittungserstellung (Bildquelle: MEDIAN-Projekt/ Bundesdruckerei/Uwe Rabeler)

Für eine statistische Auswertung müssten die Kontrollierten zusätzlich ihr Einverständnis geben, was die Transparenz weiter steigern würde. Zu diesem Zweck könnten die Betroffenen über das Online-Portal der beteiligten unabhängigen Stelle auch auf freiwilliger Basis weitere Daten eingeben, die für die statistische Auswertung von Interesse sind. Durch die nachträgliche Eingabe, auf die die Polizei keinerlei Einfluss hat, wäre auch die Freiwilligkeit gegeben.[7]

2.2 Missbrauchsrisiken vorbeugen

In der Begründung (zu Punkt 1e) weist der Antrag zutreffend darauf hin, dass die Digitalisierung der Polizeiarbeit eine konsequente Nachvollziehbarkeit der Nutzung polizeilicher Datenverarbeitungssysteme erfordert. Im

[7] Näher hierzu Bosch, Fährmann & Aden 2021.

Zuge der Ermittlungen wegen der Bedrohung von Menschen durch Schreiben eines „NSU 2.0“ wurde erneut deutlich, dass nicht immer nachvollziehbar ist, wer aus welchen Gründen Daten aus polizeilichen Systemen abfragt und nutzt. Immer wieder kommt es vor, dass mehrere Bedienstete unter derselben Kennung in polizeilichen Systemen arbeiten – obwohl dies bereits heute nach den innerdienstlichen Regelungen unzulässig sein sollte.

Die polizeiliche Datennutzung ist zumeist nur sehr allgemein an die gesetzliche Voraussetzung gebunden, dass diese für die Erfüllung polizeilicher Aufgaben erforderlich ist. Dieser gesetzgeberische Ansatz ist viel zu allgemein und verfehlt jegliche Steuerungswirkung – von Missbrauchsrisiken ganz abgesehen. Die Gesetzgebung sollte daher sowohl die tatbestandlichen Voraussetzungen der Datennutzung schärfen als auch Mechanismen einführen, die Missbrauch wirksam verhindern. Die in der Antragsbegründung erwähnten individuellen Login-Prozesse sollten daher ebenso wie die Protokollierung aller Datenbankabfragen zur gesetzlichen Pflicht gemacht werden. Wissen Polizeibedienstete, dass etwa Datenbankabfragen zu nicht-dienstlichen Zwecken untersagt sind und jederzeit nachvollzogen werden können, so dürfte dies bereits erhebliche präventive Wirkungen entfalten.

2.3. Technikfolgenabschätzung und Privacy by Design – von der Worthülse zu konkreten Anforderungen

Der Antrag lässt die Technikfolgenabschätzung unerwähnt. Dies ist nicht untypisch, da die Standards der Technikfolgenabschätzung im polizeilichen Kontext zumeist vernachlässigt werden. Die Datenschutz-Folgenabschätzung (DSFA) ist im Mai 2018 mit dem 2016 verabschiedeten EU-Datenschutzrecht für die meisten Bereiche durch den unmittelbar geltenden Art. 35 Datenschutzgrundverordnung (EU) 2016/679 (DSGVO) verbindlich geworden. Für den Teil der Polizeiarbeit, der einen Bezug zur Strafverfolgung aufweist, gilt Art. 27 der Richtlinie (EU) 2016/680, in Deutschland u.a. umgesetzt durch § 67 des Bundesdatenschutzgesetzes (BDSG). Als prozedurales Begleitelement zwingt die DSFA Unternehmen und Behörden, die Datenschutzfolgen technischer Innovationen und die

Auswirkungen auf die Grundrechte Betroffener systematisch in den Blick zu nehmen.[8]

Parlamente befassen sich in der Regel nur mit der polizeilichen Datenverarbeitung, wenn größere Investitionen anstehen, die zusätzliche Haushaltsmittel erfordern, oder wenn es in der Anwendung zu gravierenden Defiziten kommt. Behörden entscheiden im Rahmen der verfügbaren Budgets zumeist eigenständig über die Einführung und Ausgestaltung von Datenverarbeitungstechnologien. Parlamente können behördliche Datenverarbeitungsprozesse daher kaum in Gänze überschauen.[9] Daher ist eine Technikfolgenabschätzung im Vorfeld der Entscheidung über neue Formen polizeilicher Datenverarbeitung von höchster Relevanz.

Zutreffend erwähnt der Antrag in Ziffer 1a die Bedeutung der Grundsätze *privacy by design* und *privacy by default*, die gemäß Art. 25 der EU-DSGVO und Art. 20 der JI-Richtlinie (EU) 2016/680 auch für den Polizeibereich verbindlich sind. Der Grundsatz *privacy by design* besagt, dass die datenschutzkonforme Techniknutzung nicht dem Verhalten der Nutzer*innen überlassen bleiben darf, sondern durch geeignete technische und organisatorische Maßnahmen bereits während der Technikentwicklung sicherzustellen ist. Datenschutzfreundliche Sicherheitstechnologien basieren auf technischen Vorkehrungen, die dazu beitragen, Datenschutzverstöße zu erschweren oder sogar unmöglich zu machen.[10] Videoaufnahmen können z.B. ganz oder teilweise verpixelt, gespeicherte Daten einem automatisierten Löschkonzept unterworfen, Datenverarbeitungssysteme mit technisch mehrfach gesicherten Zugangssystemen versehen werden. Polizeiliche genutzte Geräte können z.B. so ausgestaltet werden, dass ein Zugriff auf Eingriffsmaßnahmen nur dann möglich ist, wenn die jeweiligen Tatbestandsvoraussetzungen erfüllt sind.[11]

Bisher beschränkt sich die gesetzgeberische Konkretisierung in der Regel auf die Wiederholung der Begriffe *privacy by design* und *privacy by default* als Worthülsen. Auch der vorliegende Antrag geht in der Konkretisierung nicht über die Forderung hinaus, diese Prinzipien „zur Maxime zu erheben“. Entscheidend ist jedoch die Definition sowohl prozeduraler als auch materieller gesetzlicher Standards, die sicherstellen, dass die Prinzipien

8 Näher hierzu Aden & Fährmann 2020.
9 Grunwald 2010, 85; Fährmann, Aden & Bosch 2020, 144; grundlegend zu den rechtswissenschaftlichen Aspekten: Roßnagel 1993.
10 Vgl. Čas 2010, 260 f.
11 Näher hierzu Fährmann, Aden & Bosch 2020; Aden & Fährmann 2020.

nicht auf der Ebene gesetzlicher Worthülsen verbleiben, sondern für die jeweiligen Anwendungsfelder zusammen mit den gesetzlichen Eingriffsvoraussetzungen konkretisiert werden.

3. Zusammenfassende Empfehlungen für die Nutzung parlamentarischer Steuerungspotenziale bei der Digitalisierung der Polizeiarbeit

Ich empfehle dem Deutschen Bundestag, im Zuständigkeitsbereich des Bundes stärker gestalterisch auf die Digitalisierung der Polizeiarbeit einzuwirken. Die strategische Ausrichtung sollte darauf abzielen, Chancen der Digitalisierung für eine effizientere und effektivere Polizeiarbeit zu nutzen, aber auch Risiken frühzeitig durch gesetzgeberische Gestaltung entgegenzuwirken. Das Parlament sollte steuernd und gestaltend auf die Verwirklichung der folgenden Ziele einwirken:

- Grundrechtsorientierte Technikfolgenabschätzung für alle Weichenstellungen bei der Digitalisierung der Polizeiarbeit;

- Sicherstellung von transparenten Abläufen zur Schaffung von Vertrauen der Betroffenen in eine faire Polizeiarbeit, etwa durch die Einführung elektronisch generierter Kontrollquittungen;

- Konkretisierung der Anforderungen an *privacy by design* und *privacy by default* durch klar konturierte gesetzgeberische Vorgaben, etwa für eine datensparsame Informationsverarbeitung und Vorgaben für eine automatisierte Menüführung polizeilicher IT-Systeme, die nur bei Vorliegen aller gesetzlichen Voraussetzungen einen Zugriff auf personenbezogene Daten und deren Verarbeitung zulässt;

- Gesetzgeberische Vorgaben für automatisierte Vorkehrungen gegen den Missbrauch polizeilicher IT-Systeme, etwa durch unberechtigte Abfragen.

Gez. Prof. Dr. Hartmut Aden

Literatur

Aden, Hartmut (2018a) Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union. In: *West European Politics*, 41(4), 981-1002.

Aden, Hartmut (2018b) ‘Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns‘ (Abschnitt N), in: Lisken, Hans (Mitgründer), Denninger, Erhard, Bäcker, Matthias & Graulich, Kurt (Hg.), *Handbuch des Polizeirechts,* 6. Aufl., München: C.H. Beck, 1617-1705 (7. Aufl. 2021 i. E.).

Aden, Hartmut (2019) Polizei und Technik zwischen Praxisanforderungen, Recht und Politik, in: *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Nr. 227, 58 (3), 7-19.

Aden, Hartmut (2020a) Interoperability Between EU Policing and Migration Databases: Risks for Privacy, in: *European Public Law*, 26(1), 93-108.

Aden, Hartmut (2020b) Transparenz als Datenschutzprinzip – Ansätze und Umsetzungsprobleme, in: *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik* Nr. 231/232, 59 (3-4), 67-75.

Aden, Hartmut & Fährmann, Jan (2020) Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, in: *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 29 (3), 24-29

Bosch, Alexander, Fährmann Jan & Aden, Hartmut (2021) Kontrollquittungen und -statistiken – Ein Instrument zur Durchsetzung des Diskriminierungsverbots bei Polizeikontrollen, in: *Zeitschrift für Kultur- und Kollektivwissenschaft* 7 (1), i. E.

Čas, Johan (2010): Privacy and Security: A Brief Synopsis of the Results of the European TA-Project PRISE, in: Serge Gutwirth, Yves Poullet und Paul De Hert, (Hg.), *Data Protection in a Profiled World*. Heidelberg: Springer, 257-262.

European Commission (2012). *Communication from the Commission to the European Parliament and the Council on strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM*), 7 December 2012, Brussels: COM(2012) 735 final.

European Data Protection Supervisor (EDPS) (2018) *Opinion 4/2018 on the Proposal for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels: EDPS.

Fährmann, Jan, Aden, Hartmut & Bosch, Alexander (2020). Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung. *Kriminologisches Journal* 52 (2): 135–148.

Grunwald, Armin (2010) Parlamentarische Technikfolgenabschätzung als Beitrag zur Technology Governance, in: Georg Aichholzer, Alfons Bora, Stephan Bröchler, Michael Decker und Michael Latzer (Hg.): *Technology Governance. Der Beitrag der Technikfolgenabschätzung.* Berlin: Edition Sigma, 85–92.

Herold, Horst (1979) Erwartungen von Polizei und Justiz an die Kriminaltechnik, in: *Kriminalistik,* 17-26.

Nogala, Detlef (1989) *Polizei, avancierte Technik und soziale Kontrolle*, Pfaffenweiler: Centaurus.

Roßnagel, Alexander (1993) *Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin*. Baden-Baden: Nomos.

Tyler, Tom R. (2017) Procedural Justice and Policing: A Rush to Judgment? *Annual Review of Law and Social Science*, 13 (1), 29–53.

Zachert, Hans-Ludwig (1991) Das Bundeskriminalamt – Gestern, Heute, Morgen. In: *Kriminalistik,* 682-687.

Stellungnahme von Dieter Schneider, Präsident Landeskriminalamt Baden-Württemberg a.D.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)863 C

Öffentliche Anhörung Ausschuss für Inneres uns Heimat am 07.06.201
Antrag der Fraktion der FDP
Smart Police – Digitalisierung der deutschen Polizei anschieben Drs. 19/27172

Vorbemerkung
Digitalisierung der deutschen Polizei ist ein sehr breites Thema mit vielen unterschiedlichen Dimensionen:
Dabei geht es z.B. um

- Ausstattung mit digitalen Arbeitsmitteln
- Digitale Kommunikationsmittel intern und extern
- Digitale Akte oder eAkte
- Digitale Forensik
- Digitales Know How
    - o für die Nutzung oder Nutzbarmachung im eigenen Aufgabenbereich,
    - o für das Verständnis der Nutzung in der Gesellschaft
    - o für die Gefahren und den Missbrauch der modernen IT
    - o um die allgegenwärtigen digitalen Spuren zu erkennen

Schwerpunkt dieser Stellungnahme ist die Digitalisierung des Informationswesens, das Informationsmanagement. Dazu folgende fünf Kernaussagen:

1. **Innere Sicherheit gewährleisten, Gefahren abwehren und Kriminalität bekämpfen setzen voraus, dass alle verfügbaren und relevanten Informationen in einem [fachlichen, technischen und organisatorischen] Gesamtsystem für die Polizeien von Bund und Ländern nutzbar sind** (Kernaussage der Saarbrücker Agenda vom 30.11.2016).
   Dieser schwergewichtigen Aussage ist uneingeschränkt zuzustimmen. Informationen sind das Kapital der Polizei, Informationen über Straftaten, Straftäter, Phänomene der Kriminalität, Entwicklungen, Gefahrenlagen und sicherheitsrelevante Umfeldfaktoren sind eine entscheidende Grundlage für gute und erfolgreiche Polizeiarbeit. Eine Beurteilung der Lage ist umso verlässlicher, je fundierter und umfassender die Faktenlage ist. Je besser die Lagebeurteilung, umso zielgerichteter sind polizeiliche Maßnahmen. – Damit sind wir wieder beim Punkt: „Jede Polizistin und jeder Polizist sollte nach Maßgabe der rechtlichen Rahmenbedingungen jederzeit und überall Zugriff auf diejenigen Informationen haben, welche für ihre/seine Aufgabenerfüllung erforderlich sind.“ Verfügbarkeit der Informationen heißt das im entsprechenden strategischen Ziel der Saarbrücker Agenda.

2. **Digitalisierung darf kein Selbstzweck sein.**
   Mit digitalen Methoden werden Strukturen und Prozesse in Organisationen nicht automatisch besser. Werden schlechte Prozesse einfach nur digitalisiert, haben Sie anschließend schlechte digitale Prozesse. Also sind vorgeschaltet der Digitalisierung Situation und Prozesse zu analysieren, Optimierungspotentiale zu identifizieren, um dann **optimierte** Strukturen und Prozesse zu digitalisieren.
   Ich empfehle Vorsicht vor Schnellschüssen mit dem scheinbaren Wundermittel Digitalisierung.
   Digitalisierung darf nicht auf ein IT-Vorhaben reduziert werden, sondern ist Teil oder auch Anstoß für eine Organisationsentwicklung. Wenn allerdings die Organisationshoheit bei 20 Teilnehmern liegt, wie beim Programm Polizei 2020, mag man erahnen, wie langwierig sich die Verständigung auf einen gemeinsamen Nenner gestalten kann.

3. **Die Umsetzung der Saarbrücker Agenda ist fachlich hoch anspruchsvoll und im föderalen Kontext extrem komplex.**
   Die Herausforderungen für die Kriminalitätsbekämpfung und Abwehr von Gefahren haben in den letzten Jahrzehnten permanent zugenommen. Die Sicherheitsorgane haben darauf mit angepassten Konzepten und Programmen spezifisch reagiert. Kernelement ist dabei jeweils das Informationsmanagement. So sind über die Jahre unzählige (Sonder-)Meldedienste, Falldateien, Auswerteprojekte u.a. entstanden, jedes für sich einleuchtend, in der Summe ist daraus jedoch ein Flickenteppich der Informationsverarbeitung entstanden.

Informationen werden in phänomenspezifischen Datensilos gespeichert und nicht übergreifend zusammengeführt. Datenverarbeitungssysteme, z.B. zur Vorgangsbearbeitung, reichen in ihrem Entwicklungsstand von top modern bis zur dv-technischen „Steinzeit“. Und dann kommt mit der Saarbrücker Agenda der Entschluss, wir harmonisieren und konsolidieren die polizeiliche IT-Landschaft – und bei näherer Befassung zeigt sich wenig Bereitschaft der Teilnehmer, von den gewohnten Spezifika abzuweichen und dafür gibt es zumeist auch gute Gründe.
Fakt ist: Polizeiarbeit ist in deutschen Landen nicht gleich Polizeiarbeit. Das Informationsmanagement als Kernelement zu harmonisieren, ist extrem aufwändig und erfordert langwierige Abstimmungen. Und dabei darf kein Teilnehmer abgehängt werden, sonst ist der Informationsverbund lückenhaft.
Zweites Problemfeld: Die „Operation Harmonisierung“ muss am lebenden Organismus am offenen Herzen erfolgen. Ein Shutdown der Informationssysteme mit einem Ausfall von relevanten Informationen für die Sicherheitsarbeit der Polizeien wäre nicht zu verantworten. Es wäre vermutlich einfacher, auf der „grünen Wiese“ eine neue Informationsarchitektur für die deutsche Polizei zu entwerfen und zu bauen und in einem Big bang einzuführen. Nach eingehender Prüfung musste diese Überlegung wegen zu großer Risiken verworfen werden.

4. **Stärkung des Datenschutzes ja, aber nicht auf Kosten der Sicherheit.**
   Stärkung des Datenschutzes durch Technik ist eines von drei strategischen Zielen der Saarbrücker Agenda und des Programms Polizei 2020. Dies wird in den Konzepten zur Umsetzung in vielfältiger Weise berücksichtigt, z.B. redundanzfreie Datenhaltung, Kennzeichnung der Daten mit dem Zweck der Erhebung, Zugriffe nach einem Rechte- und Rollenkonzept, Nutzung mit Zweckänderung nur bei vergleichbarer Ermächtigung, vollständige Protokollierung. Ein entscheidender fachlicher Mehrwert des künftigen Informationsmanagements liegt darin, dass die Verbundrelevanz von Informationen eines Teilnehmers durch das System geprüft wird. Damit kann z.B. das Auftreten eines schwarzen VW Golfs bei einem Einbruch in München, bei einer Unterschlagung an einer Tankstelle in Dresden und bei einem auffälligen Ausspähversuch einer Villa in Berlin erkannt und zusammengeführt werden. Voraussetzung ist, dass Informationen der Teilnehmer geteilt und nutzbar gemacht werden. Darüber sind weitere Gespräche und Austausche mit den Datenschutzaufsichtsbehörden zu führen, die das teilweise noch anders sehen. Der Paradigmenwechsel muss fachlich und datenschutzrechtlich vollzogen werden.

5. **Das Programm Polizei 2020 kann zu einem Erfolgsmodell werden. Die Umsetzungsgeschwindigkeit mit Zwischenzielen muss erhöht werden.**
   Nach mehr als vier Jahren seit Verabschiedung der Saarbrücker Agenda fragt man nach der Realisierung von konkreten operativen Projekten für die polizeiliche Praxis und findet noch nicht sehr viel, was tatsächlich im Wirkbetrieb umgesetzt ist.
   Die Saarbrücker Agenda war nach jahrelangen Diskussionen in den Bund-Länder-Fachgremien ein Durchbruch für das Bestreben nach Konsolidierung und Harmonisierung des Informationsmanagements. Mit der Vereinbarung des Polizei-IT-Fonds konnte in vergleichbar schneller Zeit die finanzielle Basis für ein gemeinsames Vorgehen geschaffen werden. Die Teilnehmer bringen sich zudem personell in erheblichem Umfang in die Umsetzung ein und übernehmen notwendigerweise als Themenführer Verantwortung für zahlreiche Einzelprojekte.
   Während die Anfangsphase des Programms von Grundlagenarbeit für Umsetzungsmöglichkeiten geprägt war und erfolgversprechende Herangehensweisen mangels vergleichbarer Vorhaben erst erarbeitet werden mussten, wird derzeit an mehr als 30 konkreten Einzelvorhaben intensiv gearbeitet. Das Programm ist auf dem Weg.

Ralf Michelfelder
Präsident Landeskriminalamt Baden-Württemberg a. D.
07.06.2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)863 D

Einleitung

Nachstehende Ausführungen entstanden anlässlich der

Anhörung des Innenausschusses des Deutschen Bundestags zum Antrag der Abgeordneten Benjamin Strasser u.a. und der Fraktion der FDP „Smart Police – Digitalisierung der deutschen Polizei anschieben“, BT-Drucksache 19/27172.

Die dargestellten Rahmenbedingungen und Handlungsfelder sollen lediglich exemplarisch die aktuelle Situation widerspiegeln, ohne Anspruch auf Vollständigkeit.

1. Kriminalität im Wandel

Erscheinungsformen von Kriminalität stehen immer im gesellschaftlichen Kontext, der die Rahmenbedingungen zur Straftatenbegehung bildet. Das gilt sowohl für die Art der Begehung einer Straftat als auch für Erscheinungsformen von Kriminalität. Um es vereinfacht zu sagen: Es gibt keine Postkutschenüberfälle mehr, weil es keine Postkutschen mehr gibt. Gegenläufig verhält es sich mit der Digitalisierung unserer Gesellschaft. Polizei und Gesellschaft werden mit neuen Begehungsweisen traditioneller Kriminalität, aber auch mit völlig neuen Kriminalitätsformen konfrontiert. Steigende Angriffe auf IT-Systeme korrelieren mit deren Verbreitung. Das Internet of Things (IoT), die Internetanbindung von Maschinen und Anlagen im gewerblichen und privaten Bereich, wird zunehmend weitere neue Angriffsmöglichkeiten eröffnen. Die jüngsten Ransomware Attacken auf die US Colonial Pipeline und den größten Fleischproduzenten in Südamerika haben beispielhaft vor Augen geführt, welche erheblichen Auswirkungen solche Angriffe nicht nur für das betroffene Unternehmen, aber auch in der Gesellschaft haben können.

Das Risiko, Opfer einer Straftat zu werden, beginnt heute mit dem Einschalten des PC Zuhause oder der Inbetriebnahme des Smartphones. Die Verbindung mit dem Internet ist gleichbedeutend mit dem Risiko eines bösartigen Angriffs. Zu den tradierten Parametern Opfer einer Straftat zu werden, wie Alter, soziales Umfeld, Wohngebiet etc. ist der Internetanschluss hinzugekommen. Deutlich zeigt sich dies in der Langzeitentwicklung der Kriminalität in Deutschland. Während die Straftaten insgesamt seit Jahren zurückgehen, steigt die Begehung von Straftaten mittels IT-Systemen und über das Internet rapide an, beispielsweise in Baden-Württemberg mit Steigerungsraten von jährlich über 20 Prozent in den vergangenen Jahren.[1]

[1] Sicherheitsbericht 2020 des Landes Baden-Württemberg; https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/publikationen/20210219_Sicherheitsbericht_Baden_Wuerttemberg_2020.pdf

2. Gesellschaft im Wandel

Auch unsere Sozialstruktur ist einem stetigen Wandel unterworfen. Aktuell nimmt in Deutschland die Internationalisierung der Gesellschaft zu, bis hin zu Subkulturen mit Bildung eigener Werte und Normen und dem sich Entziehen staatlicher Kontrolle. Die gesellschaftliche und wirtschaftliche Internationalisierung fördert die Bildung staatenübergreifender krimineller Netzwerke. Erfolgreiche, effiziente Polizeiarbeit muss daher reibungslos länder- und staatenübergreifend sein.

Technologischer Fortschritt hält Einzug in alle Lebensbereiche. Smarthome, Smartphone, digitale Kommunikation und Automatisierung sind alltägliche Begleiter geworden. Zirka 97,3 Prozent der 14- bis 19-jährigen Personen in Deutschland besitzen im Jahr 2020 ein Smartphone. In der Altersgruppe der 20- bis 29-Jährigen sind es 98,1 Prozent, bei den 30- bis 39-Jährigen 97,8 Prozent. Der Anteil der Smartphone-Besitzer bei den über 70-Jährigen beläuft sich immerhin noch auf 52,1 Prozent.[2] Ein Smartphone ist mehr als ein Telefon. Es ist ein Computer mit allen Office Funktionen, ein Foto mit hochauflösender Optik, eine Bank in der Hosentasche, ein Liebesbriefkasten und natürlich ein Telefon. Speichervolumen von 512 GB bis hin zu 1 TB erlauben es einem, sein ganzes Leben in der Hand oder Hosentasche zu tragen. Angesichts dieser Entwicklungen verwundert es nicht, wenn das Smartphone das einzige Internet-Gerät im Haushalt sein kann und für den Einzelnen unverzichtbar wird.

Parallel hierzu zeigt sich eine weltweite Entwicklung in der bürgerorientierten Polizeiarbeit, in welcher der Bürger zunehmend vom bloßen Konsumenten zum aktiven Teilnehmendem tendiert. Viele hochwertige Recherchetools sind online verfügbar und von jedermann nutzbar. Hohe Popularität erlangte beispielsweise bellingcat.com mit dem auf eigenen Recherchen gestützten Nachweis des Abschusses der Passagiermaschine MH-17 in der Ostukraine. Besonders interessant hierbei ist, dass sich die „Ermittler“ von bellingcat.com online staatenübergreifend vernetzten. Jede(r) bringt in dieser „internationalen Ermittlungsgruppe“ seine Kompetenz ein. So ist sich bellingcat.com sicher, den Nachweis zu führen, dass der Beschuldigte im Berliner Mordprozess z. N. des georgischen Asylbewerbers Z.K. tatsächlich eine andere Identität besitzt als die, mit der gegen ihn aktuell verhandelt wird – mit Bezügen zu staatlichen russischen Stellen.[3] Polizeiarbeit gerät in eine zunehmend kritische Wahrnehmung und Kontrolle, in der sowohl die Art des Einschreitens als auch das Ergebnis nachgeprüft und nachprüfbar werden.

Sinkende Hemmschwellen zur Gewaltanwendung gegenüber Einsatz- und Rettungskräften, Mobilisierung großer Menschenmengen zu Protestveranstaltungen, Auswirkungen ausländischer Ereignisse auf das Demonstrationsgeschehen in Deutschland, Großveranstaltungen etc. erfordern vielfach länderübergreifende Unterstützungseinsätze der Sicherheitsbehörden der Länder und des Bundes. Gleichermaßen kooperieren die Polizeien entweder auf regelmäßiger Basis (z. B. Gemeinsame Ermittlungsgruppen Rauschgift oder Schleuser) oder in anlassbezogenen Ermittlungsgruppen. Um reisende Täter

[2] https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/
[3] https://www.bellingcat.com/news/2021/03/19/berlin-assassination-new-evidence-on-suspected-fsb-hitman-passed-to-german-investigators/

erfolgreiche ermitteln zu können, müssen Tatzusammenhänge und Erkenntnisse in einzelnen Bundesländern zeitnah und umfassend zusammengefasst und der Sachbearbeitung zugänglich gemacht werden.

3. Auswirkungen auf den polizeilichen Alltag

Die gesellschaftliche Durchdringung der Digitalisierung hat mittlerweile alle Lebens- und Arbeitsbereiche erreicht. Für die Polizei ergibt sich dementsprechend die Herausforderung, mit dieser Entwicklung Schritt zu halten, um auch zukünftig weiterhin erfolgreich Gefahren abwehren und Straftaten verfolgen zu können. Dabei bestimmt nicht die Polizei das Tempo der Transformation, sondern muss selbst diesem folgen.

Erfolgreiche Polizeiarbeit heute und noch mehr in der Zukunft hängt wesentlich von der IT-Kompetenz und IT-Ausstattung der Polizei ab. Es muss also in erster Linie darum gehen, die Polizeibediensteten in der Digitalisierung zu befähigen. Dazu zählt sowohl die Kenntnis über die IT-basierten Ermittlungsmöglichkeiten, aber gleichermaßen auch die Sensibilität, an einem polizeilichen Sachverhalt das Potenzial für digitale Ermittlungsschritte zu erkennen. Digitale Spuren dominieren die polizeiliche Arbeit. Es gibt heute keinen Tatort mehr, an dem nicht digitale Spuren anfallen. Zur herkömmlichen haptischen, analogen Tatortarbeit ist die digitale hinzugekommen. Beispiele:

- Kamen früher Schraubendreher oder Brecheisen zum Einsatz, um eine Haus- oder Autotür zu öffnen, so kann dies heute über die Überwindung IT-basierter Schließsysteme erfolgt sein.
- Es gibt keine Durchsuchung, bei der nicht auch digitale Spurenträger zur Auswertung anfallen. Sei es ein Handy, ein USB-Stick, eine mobile Festplatte, ein Laptop oder ein PC. Oder alles zusammen.
- Automobile sind längst mit der viel diskutierten „Blackbox“ ausgestattet. Viele Steuergeräte speichern für Ermittlungen relevante Informationen.
- Behördliche und private Kamera, Handyvideos etc. liefern wichtige Hinweise zur Täteridentifizierung. Das bayrische Landeskriminalamt hat im Jahr 2020 insgesamt 649 Tatverdächtige über ein digitales Gesichtserkennungsprogramm identifiziert. 2013 identifizierte das bayrische Landeskriminalamt im gesamten Jahr lediglich 45 Tatverdächtige über Gesichtserkennung. [4]
- Teilautonome Videoüberwachungssysteme wie in Mannheim[5] können tatkritische Situationen erkennen und das Bild erst dann zur Verifizierung freischalten. Dies entlastet den Beobachter und stärkt den Datenschutz.
- Angesichts von Millionen ge- oder verfälschter Ausweisdokumente in der EU kann künstliche Intelligenz dazu beitragen, Fälschungsmerkmale sicher zu erkennen und darauf basierende teilautomatisierte Gutachten erstellen.

[4] Schwäbisches Tagblatt, 05.06.2021, Verbrechen auf der Spur.
[5] https://www.mannheimer-morgen.de/themen-schwerpunkte_dossier,-videoueberwachung-in-mannheim-_dossierid,118.html

Zwangsläufig noch deutlicher wird der Bedarf bei der Bekämpfung der größtenteils ausschließlich digitalen Cyberkriminalität. Um hier erfolgreich ermitteln zu können, bedarf es Experten ihres Fachs, die neben der eigentlichen Ermittlungsarbeit auch einen hohen Fortbildungsbedarf haben, um mit den Tätern Schritt halten zu können.

Alle vorstehend genannten Beispiele haben gemein, dass bei der Sicherung digitaler Spuren Unmengen an Daten anfallen, die der Aufbereitung und Auswertung bedürfen. Durchsuchungsmaßnahmen mit der Sicherung von Datenträgern im Gigabyte-Umfang sind längst üblich und werden mittlerweile von Terrabyte-Festplatten, SD-Karten und USB-Sticks verdrängt. In einem Ermittlungsverfahren des Landeskriminalamts Baden-Württemberg wurde eine Datenmenge von 1,2 Petabyte gesichert. 1 Petabyte an Text bedeutet ausgedruckt einen DIN-A4 Papierstapel mit 50.000 km Höhe. Händisches durchblättern ist hier nicht mehr drin. Ein deutscher Autohersteller hat für die Forschungsbereich autonomes Verfahren einen Datenspeicher von über 240 Petabyte verfügbar. Das entspricht einer 80 qm Wohnung mit 3 Meter Raumhöhe, vollgestopft mit CDs. Parallel zur Vergrößerung des Speichervolumens von Datenträgern werden immer mehr Daten in der Cloud abgelegt. Für die Sicherheitsbehörden ergeben sich hierdurch Herausforderungen, die bereits bei der Sicherung und Übertragung der Daten beginnen, mit deren Aufbereitung fortschreiten, bis hin zu deren Auswertung.

Bei länderübergreifenden Ermittlungsverfahren müssen ggf. diese Datenmengen in gemeinsamen Systemen zusammengeführt und erneut auf Übereinstimmungen und ergänzende Informationen analysiert werden. Zuvor bedarf es oftmals erheblicher Anstrengungen für deren Aufbereitung.

Smart Cities[6] können im Verbund mit der Polizei zu einem sicheren Leben beitragen und die Aufgabenerledigung der Polizei effizienter gestalten, wenn die Systeme miteinander kommunizieren können.

4. Polizei 2020

In ihrer Herbstkonferenz am 30.11.2016 hatten die Innenminister und Senatoren von Bund und Ländern in Saarbrücken die Schaffung einer gemeinsamen, modernen und einheitlichen Informationsarchitektur der Polizei beschlossen. Ziel ist, dass alle relevanten Informationen in einem fachlichen, technischen und organisatorischen Gesamtsystem für die Polizeien in Bund und Ländern nutzbar sind. Künftig soll beispielsweise jeder Polizeibeamte jederzeit und überall über die für ihn relevanten Informationen verfügen können. Polizeiliche IT-Angebote, die Bund und Länder betreffen, sollen nur einmal entwickelt und allen Nutzern in Bund und Ländern zur Verfügung gestellt werden. Dies verbunden mit technischen Lösungen zur Stärkung des Datenschutzes. Das auf diesem Beschluss fußende Bund-Länder Projekt trägt den Titel Polizei 2020 und steht unter der Leitung des Bundesministeriums des Innern.

[6] https://www.bmi.bund.de/DE/themen/bauen-wohnen/stadt-wohnen/stadtentwicklung/smart-cities/smart-cities-node.html

Wesentlicher Bestandteil der vorstehend genannten Grundsätze von Polizei 2020 ist die Philosophie, dass neue Anwendungen von einem oder mehreren entwickelt, aber allen zur Verfügung gestellt werden. Aktuell trägt diese Idee beispielsweise in der in Baden-Württemberg initiierten Entwicklung eines umfassenden Asservatenmanagementsystems Früchte, ebenso in einem bundesweit einheitlichen polizeilichen Fallbearbeitungssystems (eFBS), das vom Bund und dem Landeskriminalamt Baden-Württemberg als Vertreter der Länder umgesetzt wird. Das bayrische Landeskriminalamt hat die Federführung in der Beschaffung einer neuen Auswerte- und Analysesoftware für die Polizei.

Auf weitere Ausführungen hierzu verzichte ich, angesichts der vorgesehenen Anhörung von Experten zum strategisches Controlling Polizei 2020.

5. Handlungsbedarf – Digitalisierung anschieben

Weiteren Handlungsbedarf im Sinne des Antrags sehe ich in

- Entwicklungsprozesse beschleunigen
  Der vorstehend aufgeführte Ansatz von Polizei 2020 ist richtig und muss weiterverfolgt werden. Allerdings sind die derzeitigen Zeitläufe von der Bedarfsfestlegung bis zur Realisierung von oftmals fünf und mehr Jahren völlig inakzeptabel. Dabei verschlingen nicht Fragen der polizeitaktischen oder technischen Ausgestaltung, sondern das Vergabeverfahren einen Großteil der Zeit, oftmals über zwei Jahre. Bei IT-Anwendungen für die Polizei handelt es sich um Angelegenheiten der nationalen Sicherheit. Es müssen hier dringend Wege gefunden werden, um IT-Beschaffungen zu beschleunigen. Polizeiliche IT-Anwendungen sind Angelegenheiten der nationalen Sicherheit und bedürfen einer entsprechenden Priorisierung.

  Dazu gehört meines Erachtens auch das Bekenntnis, vorrangig Software von der Stange zu beschaffen, statt zeit- und kostenintensiver Maßschneiderei.

- Datenflut beherrschbar machen – Künstliche Intelligenz nutzen
  Die Polizei muss IT-Entwicklungen und deren Auswirkungen auf die polizeiliche Arbeit frühzeitig mit ihren Partnern, insbesondere den Staatsanwaltschaften abstimmen. Die exponentielle Zunahme an Daten birgt das Risiko einer für alle Beteiligten unverhältnismäßigen und unzumutbaren Auswertedauer. Niemand wäre in der analogen Welt beispielsweise auf die Idee gekommen, in einem Wirtschaftsstrafverfahren neben Umzugskartons voll mit Leitzordnern der Buchhaltung auch noch die Fotoalben des Chefs sicherzustellen und auszuwerten. Genau das aber passiert in der digitalen Welt. Es braucht daher Absprachen zwischen Staatsanwaltschaft, Ermittler und forensischer IT zum Umfang der Datenaufbereitung.

  Insbesondere bei Routineaufgaben kann künstliche Intelligenz wesentlich dazu beitragen, schnellere und personalschonende Ergebnisse zu erzielen. Diese Potenziale sind breiter nutzbar zu machen.

- Grundwissen und Expertenwissen vermitteln
  Erfolgreiche polizeiliche Digitalisierung beginnt an der polizeilichen Basis vor Ort. Was dort nicht festgestellt und gesichert wird kann auch nicht ausgewertet und weiterverarbeitet werden. Daher muss als Basiswissen gleichermaßen die Kenntnis zu den IT-Anwendungen vorhanden sein, als auch die Sensibilität für die Präsenz digitaler Spuren. Die polizeilichen Lehrpläne müssen entsprechend angepasst werden. Digitalisierung ist nicht nur eine Frage der technischen Ausstattung, sondern insbesondere auch ein Transformationsprozess für die Anwender.

  Über das Basiswissen hinaus muss IT-forensisches Expertenwissen verstärkt vermittelt werden. Spezielle Studiengänge für Cyberkriminalisten können polizeiintern, aber auch in Kooperation mit Externen angeboten werden. Für effiziente Datenanalyse braucht es in diesem Aufgabenfeld routinierte Spezialisten. Analysespitzen können über In-House Kooperation mit Fachfirmen abgedeckt werden. Externe Analyse und Auswertung sollte angesichts sensibler Daten vermieden werden.

- Die Rahmenbedingungen für performante Anwendungen schaffen
  Die Digitalisierung gewinnt dann Akzeptanz, wenn sich spürbare Vorteile für den Ermittler an der Basis zeigen. IT-Anwendungen müssen vor Ort schnell und zuverlässig zur Verfügung stehen mit einem akzeptablen Antwort-Zeitverhalten.

- Verlässliche Budgets für IT-Forensik
  Parallel zur exponentiellen Fortentwicklung der IT in Wirtschaft und Gesellschaft bedarf es einer ständigen Adaption der polizeilichen forensischen Anwendungen sowie der Speicherkapazitäten. Dies kann am sichersten über eigenständige Budgets realisiert werden.

- Zeitgemäße Ausstattung
  Die digitale Ausstattung muss Zentralstellen und Vor-Ort Dienststellen gleichermaßen umfassen. Wenn Bürgerinnen und Bürger primär ihr Smartphone in nahezu allen Lebensbereichen nutzen, muss die Polizei Möglichkeiten schaffen, darauf vorhandene Beweise (Fotos, Mails etc.) vor Ort forensisch zu sichern.

Gez.

Ralf Michelfelder