

Hartmut Aden

## Polizei und Technik zwischen Praxisanforderungen, Politik und Recht

Die polizeiliche Nutzung neuer Technologien ist aufgrund der schnellen technischen Entwicklung seit Jahrzehnten ein Dauerthema der öffentlichen Diskussion, oft verbunden mit politischen und rechtlichen Kontroversen wie z.B. bei der Vorratsdatenspeicherung. Dieser Beitrag analysiert das Spannungsfeld zwischen Praxisanforderungen an die Nutzung moderner Technik für die Polizeiarbeit, politischen Steuerungsinterventionen und rechtlichen Grenzen der Techniknutzung, die aus den Grundrechten der Betroffenen folgen. Dabei entwickelt er die These, dass die politische Steuerung der polizeilichen Techniknutzung zumeist situativ und reaktiv erfolgt, wobei die Grundrechtsorientierung eine nur untergeordnete Rolle spielt. Das Rechtssystem stößt aufgrund der hohen Geschwindigkeit der technischen Entwicklung auf strukturelle Schwierigkeiten, weil verabschiedete gesetzliche Regelungen und neue Rechtsprechungslinien schon bald von der technischen Entwicklung überholt sein können. Faktisch werden die Ambitionen für die Nutzung moderner Technik allerdings durch die bürokratische Schwerfälligkeit von Polizeibehörden gebremst.

Im Mittelpunkt der polizeilichen Techniknutzung steht das Interesse an Informationen für die Gefahrenabwehr und für Beweis Zwecke in Strafverfahren. Darüber hinaus geht es der Polizeipraxis auch um die Vereinfachung von Arbeitsabläufen. Viele Arbeiten, die in der Vergangenheit mit viel Zeitaufwand von Menschen erledigt wurden, können jetzt von Computern übernommen oder jedenfalls beschleunigt werden. Die Polizeipraxis möchte auf dem neuesten Stand der Technik sein. Gut ausgebildete Polizeibedienstete erwarten, auch im Dienst mindestens auf demselben technologischen Niveau zu arbeiten, das im privaten Bereich heute bei den meisten Menschen zum Standard geworden ist, etwa durch die Nutzung leistungsfähiger Smartphones und Notebook-Computer.

Polizeiliche Ambitionen für die Nutzung technischer Innovationen stoßen allerdings auf Grenzen. Teils gehen diese auf die begrenzte Reaktionsfähigkeit auf neue Entwicklungen zurück – Polizeibehörden sind schwerfällige bürokratische Systeme. Teils stoßen solche Ambitionen aber auch auf rechtliche Hürden, die in einem demokratischen Rechtsstaat notwendig daraus entstehen, dass polizeiliche Techniknutzung

fast immer in Grundrechte von Menschen eingreift – mit der Folge, dass der Nutzen der jeweiligen Technik für die Sicherheit der Allgemeinheit mit den Risiken für die Grundrechte Betroffener und unbeteiligter Dritter abgewogen werden muss. Damit sind komplexe Spannungsverhältnisse zwischen dem technisch Möglichen und dem (verfassungs-)rechtlich Zulässigen vorprogrammiert. Politische Entscheidungsträger\*innen stehen vor der Herausforderung, im Spannungsfeld von Praxisanforderungen, grundrechtlichen Standards und ihren eigenen politischen Profilierungsinteressen entscheiden zu müssen. Dieser Beitrag entwickelt und begründet die These, dass die Entscheidung aus strukturellen Gründen zumeist für die polizeiliche Techniknutzung ausgeht, während die Durchsetzung grundrechtlicher Standards der Verfassungsrechtsprechung überlassen wird.

## 1. Konstellationen und Dynamik polizeilicher Techniknutzung

Die polizeiliche Techniknutzung erweist sich beim näheren Hinsehen als vielfältiges Phänomen. Polizeiliche Ambitionen, verfügbare Technik zu nutzen, bezogen sich historisch z.B. auf die Bewaffnung (vgl. z.B. Funk 1986, S. 63f.) oder auf Fahrzeuge. Wegen der starken Abhängigkeit der Polizeiarbeit von Informationen hat die polizeiliche Techniknutzung parallel zur rasanten Entwicklung der Informations-, Kommunikations- und Sicherheitstechnik in den zurückliegenden Jahrzehnten erheblich an Dynamik gewonnen.

### 1.1 Polizeiliche Reaktion auf Techniknutzung durch Straftäter und Gefahrenverursacher

Seit Jahrzehnten bemüht der polizeinahe Diskurs über Techniknutzung ein Bild, das in seiner Grundstruktur unverändert bleibt, wenn auch bezogen auf unterschiedliche Technologien: Straftäter\*innen oder Menschen, die Gefahren verursachen, nutzen modernste Technik – und die Polizei muss sich anstrengen mitzuhalten. Bereits in Zeiten früher Motorisierung erwies sich die Geschwindigkeit, mit der sich manche Straftäter bewegen konnten, für die Polizei als Problem. Die Beschaffung schnellerer Fahrzeuge auch für die Polizei erschien als logische Konsequenz.

Ein solches Wechselspiel lässt sich in der Geschichte polizeilicher Technik immer wieder beobachten: Die Ausbreitung des Telefonierens führte dazu, dass auch Straftaten vermehrt mit Hilfe dieses Kommunikationsmittels geplant oder durchgeführt wurden. Auf der polizeilichen Seite führte dies in Deutschland 1968 zur Einführung der Telefonüberwachung, die sich schon wenig später zu einer viel genutzten Ermittlungsform entwickelte (zur kontinuierlichen Erhöhung der Fallzahlen: Albrecht/Dorsch/Krüpe 2003; Aden 1998, S. 382f.). Die Veränderung der Telekommunikation im Internetzeitalter bewirkte allerdings, dass sich die auf die Analogtelefonie bezogene Ermittlung zunehmend als ineffektiv erwies. Das Abhören von Internettelefonie oder gar die Online-Durchsuchung als Überwachung der Inhalte der Computer von Zielper-

sonen entwickelte sich in Reaktion darauf zum viel propagierten Wunschziel der Polizeipraxis. Hier zeigen sich allerdings auch Grenzen der polizeilichen Techniknutzung, die sich daraus ergeben können, dass die für polizeiliche Maßnahmen genutzte Technologie (noch) nicht oder nicht mehr zur Verfügung steht.

Diese Zusammenhänge zwischen Technik, die für Straftaten genutzt wird, und polizeilicher Techniknutzung ist nicht auf Informationstechnik beschränkt. So lösten Terroranschläge, bei denen die Täter schwere Waffen verwendeten, den Wunsch nach schwereren Waffen auch im Polizeidienst aus. Technische Möglichkeiten, Spuren zu vermeiden, lösen Ambitionen aus, Gegentechnologien zu entwickeln.

## 1.2 Dynamik der Kriminal-, Sicherheits- und Waffentechnik

Der Bedeutungszuwachs polizeilicher Techniknutzung geht auch auf neuere Entwicklungsschübe der Kriminal- und Sicherheitstechnik zurück. Bereits in den 1970er Jahren entwickelte die damalige Leitung des Bundeskriminalamts (BKA) weitreichende Pläne für eine systematischere Techniknutzung und die Schaffung von Synergien durch eine Bündelung avancierter Technik beim BKA (z.B. Herold 1979). Die schnelle Entwicklung der Informationstechnik führte seither nicht nur zum Ausbau der polizeilichen Informationsverarbeitung, sondern auch zu zahlreichen weiteren Innovationen, die ohne die heute verfügbare Informationstechnik nicht möglich gewesen wären. Viele Geräte und Verfahren der Spurenanalyse, die heute in der Kriminaltechnik etabliert sind, basieren auch auf der Nutzung avancierter Informationstechnik. Prozesse, die zuvor manuell erledigt werden mussten, wurden beschleunigt oder können nun teilweise oder vollständig automatisch abgewickelt werden, so der Abgleich von neuen Fingerabdrücken mit Datenbanken. Mit der DNA-Analyse hat sich in den letzten Jahrzehnten eine weitere Technologie etabliert, die heute zu den Standardinstrumenten der Aufklärung schwerer Straftaten gehört (hierzu z.B. Beck 2015).

Zudem hat Sicherheitstechnik sowohl als Forschungs- als auch als Wirtschaftszweig erheblich an Bedeutung gewonnen. Nach den Terroranschlägen in den USA am 11. September 2001 wurde auf staatlicher Ebene und in der EU massiv in technikorientierte Sicherheitsforschung investiert (kritische Bestandsaufnahme bei Kreowski/Lye in diesem Heft). Auch Unternehmen, die zuvor vorwiegend im Bereich der militärischen Sicherheit tätig waren, entwickelten neue Geschäftsfelder in der zivilen Sicherheitstechnik.

Auch an der Bewaffnung der Polizei ist die technische Entwicklung nicht vorbeigegangen. Symptomatisch hierfür sind etwa die Elektroimpulsgeräte („TASER“), deren Einführung seit Jahren kontrovers diskutiert wird (näher Tomerius in diesem Heft). Der Trend geht dabei nicht eindeutig hin zur Nutzung weniger gefährlicher Waffen – gerade in Zeiten drohender Terroranschläge wurden vermehrt auch schwere Waffen angeschafft, z.B. Maschinengewehre. Das Risiko, dass Unbeteiligte dadurch zu Schaden kommen, steigt.

### 1.3 Moderne Informations- und Kommunikationstechnik, Datenbanken und „Big Data“

Moderne Informations- und Kommunikationstechnik hat die polizeiliche Arbeit teils spät erreicht, dann aber stark verändert. Der Zugriff auf umfangreiche Datenbestände in standardisierten Datenbanken ist heute ein prägendes Element der Polizeiarbeit. Die zugrunde liegenden Datenbanken auf Landes-, Bundes- und EU-Ebene wurden in den letzten Jahrzehnten stark ausgebaut (hierzu auch Töpfer in diesem Heft). Der Zweckbindungsgrundsatz, nach dem Daten primär nur für die Zwecke verarbeitet werden dürfen, für die sie erhoben wurden, ist in manchen Bereichen stark relativiert worden, in letzter Zeit insbesondere durch den Trend hin zu interoperablen Datenbanken in Deutschland und in der EU (näher hierzu Aden/Fährmann 2019, S. 177f.). Darüber hinaus können Polizeibehörden unter bestimmten Voraussetzungen auf Datenbestände Dritter zugreifen, etwa bei der sogenannten Rasterfahndung. Informationstechnik ist auch die Grundlage für viele kriminaltechnische Entwicklungen.

Bei der Kommunikationstechnik tun sich Polizeibehörden weiterhin schwer, im Tempo der technischen Entwicklung mitzuhalten. Die regelmäßige Ausstattung aller Polizeibediensteten mit Mobilgeräten der neuesten Generation (Smartphones, Tablets u.a.) würde manchen polizeilichen Beschaffungsetat überfordern. Die besondere Absicherung vertraulicher polizeilicher Kommunikation gegen Angriffe von außen trägt ebenfalls dazu bei, dass neue Generationen von Kommunikationstechnik nur zeitverzögert zum Einsatz kommen.

Die Verfügbarkeit großer Datenbestände, z.B. über die Standorte von Mobiltelefonbesitzer\*innen und das Suchverhalten im Internet, hat auch im polizeilichen Bereich zunehmend Begehrlichkeiten hervorgerufen. Die Vorratsdatenspeicherung, also die Aufbewahrung eigentlich nicht mehr benötigter Telekommunikations-Metadaten (Verbindungsdaten, Standorte usw.) als eine Art Ermittlungsreserve für noch nicht eingetretene Gefahren oder Straftaten, ist ein vieldiskutiertes Beispiel (s. den Beitrag von Weichert in diesem Heft).

Mit der Entwicklung „künstlicher Intelligenz“ und neuer Verfahren zur Aufbereitung großer Datenmengen sind zahlreiche (potentielle) Anwendungsfälle hinzugekommen, z.B. die automatisierte Auswertung von Videodaten, die der Polizei nach Anschlägen oder Amoktaten aus verschiedenen Quellen zur Verfügung stehen (u.a. durch die freiwillige Übermittlung privater Aufnahmen). Auch Experimente mit der Gesichtserkennung, so am Bahnhof Berlin-Südkreuz, basieren auf neuen Technologien für die Auswertung großer Datenmengen. Im Hinblick auf die Grundrechte der Betroffenen liegt die Schwäche der meisten Formen von *Big Data*-Auswertung darin, dass fast ausschließlich Daten Unbeteiligter verarbeitet werden, die mit Gefahren oder Straftaten nichts zu tun haben. *Predictive Policing* verspricht prognostische Aussagen über zu erwartende Unsicherheitsfaktoren, die ebenfalls auf der automatisierten Auswertung großer Datenmengen basieren. Validität und Nutzen hängen allerdings stark von den verwendeten Algorithmen ab (zur Kritik z.B. Ostermeier 2018; Thurn/Egbert in diesem Heft).

## 2. Verlangsamende Einflussfaktoren für die polizeiliche Techniknutzung

Verwaltungen sind zumeist keine Vorreiter der Digitalisierung. Die Innovationszyklen für die Beschaffung neuer Hard- und Software sind vergleichsweise lang. Auswirkungen unzulänglicher technischer Ausstattung auf einen effektiven Personaleinsatz werden nur selten in den Blick genommen.

Das gilt grundsätzlich auch für die Polizei. Wahlversprechen bezogen sich in den letzten Jahren oft auf die Schaffung zusätzlicher Stellen, ohne die nötigen Mittel für eine moderne Arbeitsplatzausstattung bereitzustellen. Auch die Befürchtung, durch technische Innovationen könnten Arbeitsplätze wegfallen, begrenzt Innovationen und ihre Akzeptanz bei Bediensteten und insbesondere bei ihren Gewerkschaften. In einigen Bundesländern verfügen Polizist\*innen im Streifendienst nicht über mobile Kommunikationsgeräte, die Datenbankabfragen wie am Büro-Arbeitsplatzrechner zu lassen. Daher müssen Abfragen per Funk oder Mobiltelefon an eine Leitstelle durchgegeben werden, wo ein weiterer Bediensteter die Abfragen durchführt und die Ergebnisse an die anfragenden Kolleg\*innen zurückgibt. In manchen Fällen kann dieser Vorgang sehr zeitaufwendig sein, etwa bei Namen mit komplizierter Schreibweise. Hier ist Personal gebunden, das an anderer Stelle sinnvollere Aufgaben erledigen könnte.

Trotz Verwaltungsmodernisierung sind die Entscheidungsprozesse für technische Innovationen aufwendig. Bei größeren Investitionen müssen zunächst mit Regierung und Parlament die nötigen Haushaltsmittel ausgehandelt werden. Erst dann können die förmlichen Entscheidungsprozesse über die Technologieauswahl und die bei größeren öffentlichen Beschaffungsaufträgen zwingende Ausschreibung beginnen. Bei einer sehr schnellen technischen Entwicklung sind Behörden so kaum zu einer schnellen Reaktion in der Lage.

Wurden Entscheidungen über technische Neuerungen getroffen, müssen die Beschäftigten noch von ihrem Nutzen überzeugt werden – ein Schritt, der in der Polizei und anderen Verwaltungen manchmal vernachlässigt wird. Bedienstete, die sich viele Jahre an Geräte oder Abläufe gewöhnt haben, tun sich möglicherweise schwer, sich an neue Geräte oder Software zu gewöhnen. Die frühzeitige Einbindung der Bediensteten in technische Innovationsprozesse und ihre systematische Vorbereitung auf Veränderungen (*Change Management*) sind bei Polizei und anderen Verwaltungen nicht immer gewährleistet.

## 3. Sicherheitsorientierte Entscheidungsallianzen

Auch wenn technische Innovationen im Polizeibereich wegen bürokratischer Hürden oft nur zeitverzögert ankommen, sind die politischen Rahmenbedingungen für Investitionen in Sicherheitstechnik eher günstig. Innenministerien haben ein Eigeninteresse an einer funktionierenden Gewährleistung von Sicherheit. Für Funktionsdefizite

sind sie unmittelbar verantwortlich. Um sich die Loyalität der Polizeibediensteten zu erhalten und sich gegen Sicherheitsrisiken abzusichern, liegen Investitionen in Sicherheitstechnik nahe. Jedenfalls in Phasen, die nicht zu stark von Haushaltsrestriktionen geprägt sind, haben Investitionen in Sicherheitstechnik daher gute Chancen als ein Element sicherheitsorientierten politischen Entscheidens durchgesetzt zu werden.

Nicht nur Polizeigewerkschaften, sondern auch polizeiliche Führungskräfte haben diesen Effekt durch eine gezielte Öffentlichkeitsarbeit immer wieder genutzt, um Forderungen nach einer besseren Ausstattung und mehr Eingriffsbefugnissen Nachdruck zu verleihen. Bereits in den 1970er Jahren propagierten der damalige BKA-Präsident Horst Herold und andere führende Polizeibeamte einen weitreichenden Wandel der Polizeiarbeit, für den die Technisierung ein wesentlicher Faktor war (vgl. Herold 1979; zur Kritik: Nogala 1989, S. 150f. *et passim*). Spätere BKA-Präsidenten setzten diese Linie fort (u.a. Zachert 1991).

Zudem sind technische Innovationen wie die erweiterten Möglichkeiten der Nutzung biometrischer Daten beliebte Elemente politischer Sicherheitsversprechen (zur Kritik: Kühne/Schlepper 2018). Im Ergebnis haben die sicherheitsorientierten Entscheidungssallianzen zu einer kontinuierlichen Ausweitung nicht nur der technischen Ausstattung der Polizei, sondern auch der rechtlichen Eingriffsbefugnisse geführt. Die Auswirkungen auf die Grundrechte fanden kaum Berücksichtigung, und die Schutzstandards blieben in der Regel auf das Mindestmaß des verfassungsgerichtlich geforderten Grundrechtsschutzes beschränkt (zur Kritik: Aden/Fährmann 2018 und 2019; Aden 2013). Damit ist das rechtsstaatliche Legitimationskonzept des staatlichen Gewaltmonopols, das auf gesetzlich begrenzten Eingriffsbefugnissen basiert, in eine Krise geraten (hierzu näher Bäuerle 2013).

#### 4. Rechtliche Grenzen polizeilicher Techniknutzung

Rechtliche Grenzen der polizeilichen Techniknutzung folgen vor allem aus den Grundrechten der Betroffenen. Die Gewinnung von Informationen für die Gefahrenabwehr und für Beweis Zwecke im Strafverfahren ist ein zentrales Ziel polizeilicher Techniknutzung. Daher sind vor allem die Grundrechte zum Schutz der Privatsphäre in ihren verschiedenen Dimensionen betroffen: das Telekommunikationsgeheimnis (Art. 10 GG), die Unverletzlichkeit der Wohnung (Art. 13 GG), die informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, letztere durch das Bundesverfassungsgericht abgeleitet aus Art. 1 Abs. 1 und Art. 2 Abs. 1 GG. Mit der Europäischen Menschenrechtskonvention (EMRK) und der EU-Grundrechtecharta sind diese Grundrechte in ähnlicher Form auch europaweit verankert, insbesondere in Art. 7 und 8 der Charta und Art. 8 EMRK. Politische Entscheidungsträger versuchen oft, bei der Schaffung von Eingriffsgrundlagen für polizeiliche Techniknutzung die Spielräume des gerade noch grundrechtlich Möglichen auszureizen (näher hierzu Aden & Fährmann 2018, S. 25f. und 2019, S. 176f.). Stärker am Grundrechtsschutz orientierte Parteivertreter\* innen wie sie in Teilen der FDP, bei den Grünen und der Linkspartei anzutreffen sind, haben hier in

der Regel nur eine geringe Korrektivfunktion. Da diese Parteien nur selten bzw. bisher nie Innenminister\*innen stellten, ist ihr Einfluss auf die praktische Politik innerer Sicherheit gering. Korrekturen im Interesse des Grundrechtsschutzes bleiben so vor allem den Gerichten überlassen, insbesondere dem Bundesverfassungsgericht, dem Europäischen Gerichtshof für Menschenrechte (EGMR) und dem Gerichtshof der EU (EuGH) (näher hierzu Aden 2016; Aden/Fährmann 2018 und 2019).

#### 4.1 Funktionen des Rechts für die polizeiliche Techniknutzung – zwischen Begrenzung, Legitimation und Rechtfertigung

Die Gründe und Voraussetzungen für die Befolgung von Recht sind vielfältig und ambivalent (ausführlich Friedman 2016, S. 40ff. *et passim*). Dies gilt nicht nur für Bürger\*innen, die mehr oder minder rechtstreu sind, sondern auch für Polizeibeamt\*innen, die gesetzliche Vorgaben für ihr Handeln und ihre Techniknutzung entweder als lästige Begrenzung oder als hilfreiche Handlungsanleitung begreifen können (hierzu Aden 2013).

Aus der polizeilichen Sicht sind die Wirkungen grundrechtlicher Schranken und rechtlicher Regelungen für die Techniknutzung ambivalent. Zunächst ist die *Begrenzungsfunktion* zu nennen. Aus rechtlichen Vorgaben ergeben sich Grenzen der zulässigen Techniknutzung, die von Polizeipraktiker\*innen oft als lästig empfunden und daher zum Gegenstand politischer Kampagnen gemacht werden. So kann nicht jede Information gespeichert werden, sondern in der Regel ist ein konkreter Zweck erforderlich. Kriminaltechnische Innovationen wie die Gesichtserkennung können möglicherweise nicht oder nur eingeschränkt genutzt werden, wenn sie die Grundrechte der Zielpersonen oder unbeteiligter Dritter unverhältnismäßig einschränken.

Die *Legitimation* polizeilichen Handelns steht immer dann im Mittelpunkt, wenn eine gesetzliche Grundlage die Techniknutzung erlaubt. Denn mit einer vorhandenen Rechtsgrundlage bewegt sich das polizeiliche Handeln auf sicherem Terrain (näher hierzu Aden 2013, S. 16f.). Aus polizeipraktischer Sicht ist es vorteilhaft, wenn gesetzliche Eingriffsbefugnisse eher allgemein gehalten sind, damit möglichst alle praktischen Bedarfe der Techniknutzung darunter gefasst werden können. Bereits Zweifel daran, ob eine ausreichende Rechtsgrundlage vorhanden ist, beeinträchtigen die polizeiliche Handlungssicherheit. Denn diese Unsicherheit senkt die Legitimität polizeilichen Handelns und setzt es dem Risiko externer und interner Kritik aus – bis hin zur gerichtlichen Feststellung der Rechtswidrigkeit.

Schließlich ist auch die *Rechtfertigungsfunktion* relevant. Gerade wenn die Legitimation polizeilichen Handelns angezweifelt wird, z.B. weil verfügbare Technik auf eine Weise genutzt wurde, bei der unklar ist, ob sie von den gesetzlichen Grundlagen gedeckt ist, kann das vorhandene rechtliche Repertoire genutzt werden, um eine rechtfertigende Argumentationsstrategie zu entwickeln. Eine „polizeifreundliche“ Auslegung vorhandener Gesetze kann eher als eine strikt grundrechtsorientierte Interpretation zu dem Ergebnis kommen, dass eine hinreichende Rechtsgrundlage besteht. In der Praxis ist die Rechtfertigung im Nachhinein auch in Situationen relevant, in denen unter Zeitdruck oder im Hinblick auf die schnelle und effiziente Lösung eines Si-

cherheitsproblems Technik eingesetzt wurde, ohne über die rechtlichen Grundlagen näher nachzudenken. In diesen Fällen obliegt es zumeist den Justitiariaten der Polizei, eine Argumentation zu entwickeln, nach der das Geschehene rechtlich zulässig war. Die zuständigen Gerichte haben am Ende zu entscheiden, ob diese Position rechtmäßig ist. Wird das Recht auf diese Weise genutzt, dient es allerdings nicht der rechtsstaatlichen Begrenzung von Grundrechtseingriffen, sondern der Rechtfertigung des faktischen Handelns im Nachhinein. Gelingt es einer solchen Rechtfertigung, die Betroffenen davon zu überzeugen, dass die Polizei richtig gehandelt hat, mag das Handeln im Sinne eines Rechts auf Rechtfertigung (vgl. Forst 2007) als gerecht empfunden werden. In einem Rechtsstaat erfüllen polizeiliche Eingriffsbefugnisse aber zusätzlich eine handlungsanleitende und -begrenzende Funktion für die Polizei, die eine verfassungsgemäße Rechtsgrundlage bereits zum Zeitpunkt des Entscheidens über das polizeiliche Handeln, also z.B. über den Einsatz einer bestimmten Technik, voraussetzt.

#### 4.2. Langsames Recht, dynamische Technikentwicklung und Zonen der Informalität

Die Legitimation polizeilicher Techniknutzung durch gesetzliche Eingriffsgrundlagen ist nicht statisch, sondern hängt eng mit der technischen Entwicklung zusammen. Die rechtlichen Regelungen müssen kontinuierlich an die technische Entwicklung angepasst werden, je nach Tragweite durch interpretierende Rechtsprechung oder durch Gesetzgebung. Das Rechtssystem ist an rechtsstaatliche Verfahrensabläufe gebunden. Rechtsprechung und Gesetzgebung sind daher langsam – nicht nur im Vergleich zur technischen Entwicklung, sondern auch zum politischen System, das stärker auf ad-hoc-Entscheidungen zurückgreifen kann und muss, um akut anstehende Probleme zu lösen (ausführlich Luhmann 1995, S. 427 *et passim*).

Die technische Entwicklung ist somit ihrer rechtlichen Einhegung tendenziell stets voraus. Dies kann verschiedene Konsequenzen haben. Kommt neue Technik zum Einsatz, fehlt es möglicherweise an rechtlichen Regelungen. In der Praxis besteht dann eine Verunsicherung darüber, ob vorhandene technische Möglichkeiten genutzt werden können, z.B. bei der Geolokalisierungstechnik, die wie z.B. das *Global Positioning System* (GPS) mit Satellitentechnik den Standort mobiler Geräte weitgehend genau berechnen kann. Ihre Nutzungsmöglichkeiten haben sich mit der Verbreitung mobiler Kommunikationsgeräte stark weiterentwickelt (näher hierzu Aden/Fährmann in diesem Heft). Eine rechtswissenschaftliche Technikfolgenforschung (im Sinne von Roßnagel 1993) kann die daraus entstehenden Steuerungsdefizite abmildern, aber nicht gänzlich vermeiden.

Technische Entwicklungen können auch dazu führen, dass Technikeinsatz, der zuvor noch rechtlich zulässig war, neue Rechtsgrundlagen erfordert oder sogar ganz oder teilweise unzulässig wird. Ein viel diskutiertes Beispiel ist die polizeiliche Nutzung von Videotechnik. Lange Zeit wurde die Auffassung vertreten, die Nutzung von Übersichtsaufnahmen sei kein Grundrechtseingriff, da auf diesen Aufnahmen niemand konkret zu erkennen sei. Mit der Entwicklung der Videotechnik ist diese Argumentation allerdings hinfällig geworden. Marktübliche Videotechnik verfügt über



eine hohe Auflösung und über vielfältige Möglichkeiten des Zoomens von Bildausschnitten. Damit wuchsen auch die Begehrlichkeiten, diese Technologie für die polizeiliche Fahndung und Beweisgewinnung in Ermittlungsverfahren zu nutzen. In Kombination mit Software zur Gesichtserkennung entstehen gänzlich neue Fahndungsmöglichkeiten. Verfahren zur automatisierten Auswertung großer Mengen an Videomaterial werden derzeit erforscht. Durch diese Entwicklungen ist die Videotechnik allerdings auch im Hinblick auf die Intensität der ermöglichten Grundrechtseingriffe völlig neu zu bewerten. Die technologischen Möglichkeiten zur Erfassung der Bewegungen des Menschen im öffentlichen Raum sind so stark gewachsen, dass vorsichtige Menschen vom Gebrauch ihrer Grundrechte abgehalten werden könnten. Dies gilt auch, aber nicht nur für die Teilnahme an Demonstrationen. Neben rechtlichen Begrenzungen durch hohe Tatbestandsvoraussetzungen und Verhältnismäßigkeitsanforderungen sind – im Sinne von *Privacy by Design* – auch technische Lösungen erforderlich, die eine grundrechtsschonende Techniknutzung sicherstellen.

Eine weitere Variante sind eingespielte Formen polizeilicher Techniknutzung, die aufgrund neuer technischer Entwicklungen nicht mehr oder nur noch eingeschränkt nutzbar sind. So wird von der Polizeipraxis vielfach beklagt, dass die Telefonüberwachung, die sich seit den 1960er Jahren zu einer der praxisrelevantesten Ermittlungsstrategien entwickelt hatte, aufgrund der Umstellung auf internetbasierte Telefonie nur noch eingeschränkt eingesetzt werden kann. Denn die Überwachungstechnologie nutzte den Zugriff an zentralen Vermittlungsknoten. Bei der internetbasierten Telekommunikation fehlt es indes an solchen zentralen Zugriffspunkten. Zudem ist die Kommunikation zunehmend verschlüsselt. Der staatliche Zugriff ist nur über das Endgerät der Nutzer\*innen möglich und daher mit wesentlich intensiveren Grundrechtseingriffen verbunden als das frühere Abhören leitungsgebundener Kommunikation (zum Diskussionsstand: Petri 2018, Rn. G 680ff.).

Die schnelle Entwicklung der Technik führt in manchen Fällen zu einer Techniknutzung in Zonen rechtlicher Informalität. Dies ereignet sich immer dann, wenn noch unklar ist, ob und ggf. wie eine neue Technologie grundrechtskonform polizeilich genutzt werden kann oder wenn die technische Entwicklung die Eingriffsintensität vorhandener Technologien schleichend erhöht. Häufig neigen Praxisakteure in solchen Situationen dazu, verfügbare Technik erst einmal zu nutzen – hoffend, dass diese Praxis später durch die Rechtsprechung für zulässig erklärt oder durch neue Gesetze legitimiert wird. Das Risiko für die handelnden Beamt\*innen ist gering, da ihr Vorgehen aufgrund der rechtlichen Unsicherheit nicht eindeutig rechtswidrig ist – disziplinar- oder gar strafrechtliche Konsequenzen sind daher in solchen Fällen unwahrscheinlich.

Wurde die Nutzung polizeilicher Technik – jedenfalls in gewissen Grenzen – durch Rechtsprechung oder Gesetzgebung „abgesegnet“, kann dies weitreichende Folgen haben. Die Praxis wird so ermutigt, die betreffenden technischen Möglichkeiten auch zu nutzen. Legalistisch eingestellte Polizeibedienstete haben nun keine Gründe, bei der Nutzung einer Technik zu zögern. Politische Forderungen nach der Finanzierung für die jeweilige Technologie haben so besonders gute Realisierungschancen. Einmal rechtlich legitimierte Polizeitechnik wird daher absehbar wesentlich stärker genutzt als zuvor.

### 4.3 Synergien zwischen Grundrechtsschutz und effektiver polizeilicher Techniknutzung: zielgerichtete statt massenhafte Datenhaltung und Verbesserung der Datenqualität

Grundrechtsschutz und effektive polizeiliche Sicherheitsgewährleistung durch Techniknutzung sind keine so großen Gegensätze, wie dies von Innenpolitiker\*innen und Polizeipraxis manchmal suggeriert wird. Denn rechtliche Vorgaben lenken die Techniknutzung nicht nur in rechtsstaatliche, sondern oft auch in effektivere Bahnen.

Der Umgang mit „Big Data“ ist hierfür ein instruktives Beispiel. Sicherheitsbehörden tendieren oft dazu, große Datensammlungen „auf Vorrat“ für ein zentrales Instrument moderner Techniknutzung zu halten. Dabei wird allerdings übersehen, dass größer werdende Datenmengen allein kaum effektiv zu mehr Sicherheit beitragen können. Entscheidend ist vielmehr die Qualität der Daten. Sie müssen zweckdienlich, aktuell und zutreffend sein. Genau dies sind die Anforderungen des Grundrechtsschutzes, der Sicherheitsbehörden nur die Verarbeitung korrekter personenbezogener Daten erlaubt. Grundrechtsbezogene Verarbeitungsregeln zwingen Sicherheitsbehörden damit auch zu einem effektiveren Umgang mit massenhaft verfügbaren Informationen. Allerdings sind Sicherheitsbehörden noch nicht darauf eingestellt, die Qualität ihrer Datenbestände regelmäßig zu prüfen, Fehlerhaftes zu korrigieren und Veraltetes zu löschen (näher hierzu Aden 2018, S. 995ff.). Das neue EU-Datenschutzrecht, hier die für weite Teile der Polizeiarbeit geltende Richtlinie (EU) 2016/680, könnte das Umdenken beschleunigen. Technische Voreinstellungen für die Löschung und Qualitätssicherung im Sinne von *Privacy by Design* liefern hierfür wichtige Ansatzpunkte (hierzu auch Aden/Fährmann 2019, S. 178).

Kritische Analysen der jüngeren Entwicklung des Polizei- und Strafprozessrechts sind sich darin einig, dass die Art und Weise, wie Technik im Polizeibereich genutzt wird, mit der Vorverlagerung polizeilicher Kompetenzen weit in das Vorfeld von Gefahren und Straftaten verknüpft ist. Mehr oder minder konkrete Präventionskonzepte prägen heute weite Teile der polizeilichen Arbeit. Wenn diese Konzepte bereits Grundrechte nur potentiell verdächtiger oder gefährlicher Personen oder gar unbeteiligter Dritter beeinträchtigen, ist diese Vorverlagerung aufgrund der mit ihr verbundenen Grundrechtseingriffe nicht verhältnismäßig und daher unzulässig (näher hierzu Aden/Fährmann 2018 und 2019 m.w.N.). Dies ist der Kern vieler polizei- und rechtspolitischer Auseinandersetzungen über die Nutzung des technisch Möglichen, etwa im Zusammenhang mit der Vorratsdatenspeicherung.

## 5. Ausblick – weitere Technisierung durch „Big Data“ und „Künstliche Intelligenz“

Dieser Beitrag hat gezeigt, dass die Technisierung der Polizeiarbeit ein dynamischer und zugleich ambivalenter Prozess ist. Einerseits liegt es nahe, dass auch Sicherheitsbehörden mit moderner Technik ausgestattet werden, um ihre Aufgaben effektiv und effizient bewältigen zu können. Andererseits führt diese Technisierung zu Grundrechtseinschränkungen, auch weil die polizeilichen Kompetenzen im Vorfeld von Gefahren und Straftaten erheblich ausgeweitet wurden.

Absehbar ist dieser ambivalente Wechselwirkungsprozess zwischen Technikentwicklung, polizeilicher Techniknutzung und grundrechtsschonender Einhegung nicht abgeschlossen. Die Verfügbarkeit großer Datenmengen, die Menschen heute durch die Nutzung mobiler Geräte und vernetzter Anwendungen als Spuren hinterlassen, dürfte weiter zunehmen, insbesondere wenn mit dem „Internet der Dinge“ weitere alltäglich genutzte Geräte vernetzt werden. Auch die viel diskutierte „künstliche Intelligenz“ ist längst in der Forschung zur Sicherheitstechnik angekommen und wird bereits bei der Entwicklung des *Predictive Policing* und anderer Formen von Auswertung großer Datenmengen genutzt. Auch hier stoßen Chancen für eine effektivere Gewährleistung von Sicherheit auf neue Risiken für die Grundrechte, wenn Lagebewertungen und die daraus zu ziehenden Konsequenzen zukünftig von Maschinen auf der Basis sich selbst weiterentwickelnder Algorithmen getroffen oder jedenfalls vorbereitet werden.

**PROF. DR. HARTMUT ADEN** ist Jurist und Politikwissenschaftler. Er ist Professor für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft an der Hochschule für Wirtschaft und Recht Berlin, dort stellv. Direktor des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS) sowie behördlicher Datenschutzbeauftragter der Hochschule. Webseite: [www.hwr-berlin.de/prof/hartmut-aden](http://www.hwr-berlin.de/prof/hartmut-aden).

## Literatur

Aden, Hartmut 1998: Polizeipolitik in Europa. Wiesbaden: Westdeutscher Verlag.

Aden, Hartmut 2013: Polizei und das Recht: Stressquelle oder Stressvermeidung? In: Rainer Prätorius & Lena Lehmann (Hg.), *Polizei unter Stress?*, Frankfurt/Main: Verlag für Polizeiwissenschaft, S. 15-34.

Aden, Hartmut 2016: Wie beeinflusst der Gerichtshof der EU die Politik öffentlicher Sicherheit? Mehr Freiheit oder mehr Sicherheit? In: Britta Rehder & Ingrid Schneider (Hg.), *Gerichtsverbände, Grundrechte und Politikfelder in Europa*, Baden-Baden: Nomos, S. 233-258.

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

Aden, Hartmut & Fährmann, Jan 2018: Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, Gutachten und Vorstudie, Berlin: E-Paper der Heinrich Böll Stiftung, Berlin: Dezember 2018 [https://www.boell.de/sites/default/files/endf\\_e-paper\\_polizeirecht\\_vereinheitlichen.pdf?dimension1=division\\_demo](https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf?dimension1=division_demo) (zuletzt geprüft am 19.10.2019).

Aden, Hartmut & Fährmann, Jan 2019: Defizite der Polizeirechtsentwicklung und Techniknutzung. In: *Zeitschrift für Rechtspolitik (ZRP)* 52 (6), S. 175-178.

Albrecht, Hans-Jörg, Dorsch, Claudia & Krüpe, Christiane 2003: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Eine rechtstatsächliche Untersuchung im Auftrag des Bundesministeriums der Justiz, Freiburg im Breisgau: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Bäcker, Matthias 2015: *Kriminalpräventionsrecht*, Tübingen: Mohr Siebeck.

Bäuerle, Michael 2013: Strukturelle Grenzen von Steuerung und Kontrolle der Polizei in der Demokratie. In: *vorgänge* 52 (4), Heft 204, S. 29-40.

Beck, Maren 2015: *Die DNA-Analyse im Strafverfahren: de lege lata et ferenda*, Baden-Baden: Nomos.

Forst, Rainer 2007: *Das Recht auf Rechtfertigung. Elemente einer Theorie der Gerechtigkeit*, Frankfurt/Main: Suhrkamp.

Friedman, Lawrence M. 2016: *Impact. How Law Affects Behavior*, Cambridge, MA: Harvard University Press.

Funk, Albrecht 1986: *Polizei und Rechtsstaat. Die Entwicklung des staatlichen Gewaltmonopols in Preußen 1848-1914*, Frankfurt/Main: Campus.

Garland, David 2001: *The Culture of Control. Crime and Social Order in Contemporary Society*, Oxford & New York: Oxford University Press.

Herold, Horst 1979: Erwartungen von Polizei und Justiz an die Kriminaltechnik. In: *Kriminalistik*, S. 17-26.

Kühne, Sylvia & Schlepper, Christina 2018: Zur Politik der Sicherheitsversprechen. Die biometrische Verheißung. In: Jens Puschke & Tobias Singelstein (Hg.), *Der Staat und die Sicherheitsgesellschaft*, Wiesbaden: Springer VS, S. 79-99.

Luhmann, Niklas 1995: *Das Recht der Gesellschaft*, Frankfurt/Main: Suhrkamp.

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

Ostermeier, Lars 2018: Der Staat in der prognostischen Sicherheitsgesellschaft. Ein technografisches Forschungsprogramm. In: Jens Puschke & Tobias Singelstein (Hg.), *Der Staat und die Sicherheitsgesellschaft*, Wiesbaden: Springer VS, S 101-121.

Petri, Thomas 2018: *Informationsverarbeitung im Polizei- und Strafverfahrensrecht*. In: Hans Liskens (Mitbegründer), Erhard Denninger, Matthias Bäcker & Kurt Graulich (Hg.), *Handbuch des Polizeirechts*, 6. Aufl., München: C.H. Beck, S. 885-1058.

Roßnagel, Alexander 1993: *Rechtswissenschaftliche Technikfolgenforschung. Umriss einer Forschungsdisziplin*. Baden-Baden: Nomos.

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