Deutsche Hochschule
der Polizei
Universität der Polizeien
des Bundes und der Länder

Die Entwicklung der Polizeitechnik im 21. Jahrhundert

Herausgegeben von Wilfried Honekamp und Gundula Gahlen

Band
31

Schriftenreihe
der Deutschen Hochschule der Polizei

Schriftenreihe
der Deutschen Hochschule der Polizei
neue Folge

Band 31

hrsg. vom Kuratorium der Deutschen Hochschule der Polizei

Deutsche Hochschule
der Polizei
Universität der Polizeien
des Bundes und der Länder

Die Entwicklung der Polizeitechnik im 21. Jahrhundert

Herausgegeben von Wilfried Honekamp
und Gundula Gahlen

Münster, 2026

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung vorbehalten.

Fachbeirat:

Kriminaldirektor im Hochschuldienst Joachim Faßbender
Prof. Dr. Thomas Görgen
Prof. Dr. Stefan Jarolimek
Prof. Dr. Anja Schiemann
Prof. Dr. Dr. Antonio Vera

© Deutsche Hochschule der Polizei – Hochschulverlag
Zum Roten Berge 18–24
48165 Münster
ISBN 978-3-945856-33-8
ISSN 1865-0430

Inhaltsverzeichnis

7 **Strukturwandel der Polizeitechnik im 21. Jahrhundert – Entwicklungslinien und interdisziplinäre Perspektiven**
Wilfried Honekamp und Gundula Gahlen

15 **Europa- und verfassungsrechtliche Anforderungen an die polizeiliche Datenverarbeitung beim Einsatz automatisierter und KI-gestützter Systeme**
Dirk Kunze

32 **Die Entwicklung der polizeilichen Presse- und Öffentlichkeitsarbeit – Von Brief und Fax bis zum crossmedialen Kommunikationsmanagement und zur Professionalisierung der Mitarbeitenden**
Stefan Jarolimek

46 **Digitale Forensik nach Ernst Gennat – Methodisches Denken im Zeitalter digitaler Spuren**
Dirk Labudde und Roman Povalej

61 **Automatisierung bei der Polizei – Von der Rasterfahndung über POLAS-Sammelabfragen bis zum Einsatz Künstlicher Intelligenz: vom Bürgerpolizisten zum Technikbeiwerk?**
Andreas Beier

77 **Von der Insellösung zur Datenplattform: Entwicklungslinien polizeilicher Datenarchitekturen seit 2000 und ihre organisatorischen Folgen**
Anosch Amanat

96 **Digitale Fahrzeugdaten als Entwicklungslinie moderner Polizeitechnik – Rechtliche Leitplanken und praxisnahe Nutzung im digitalen Zeitalter**
Andreas Mehlich und Kilian L. Scholz

114 **Vom Datenträger zur Cloud – Die Entwicklung der digitalen Forensik in der Polizeiarbeit**
Heiko Rittelmeier

132 **Der digitale Zwilling in der Forensik – Entstehung, Entwicklung und Bedeutung für die Polizeitechnik**
Dirk Labudde

148 **Von MS Paint bis Deepfakes – Digitale Fälschungen seit 2000 als Herausforderung für Polizei und Forensik**
Robert Diedrich Ulrich Lippitz

171 **Von Computerkriminalität zu Cybercrime – Die Entwicklung im 21. Jahrhundert**
Wilfried Honekamp

191 **Polizeihochschulen als Schnittstellen technischer Transformation**
Johannes Fähndrich und Wilfried Honekamp

Inhaltsverzeichnis

200 **Die Bedeutung von Technischen Richtlinien für Einsatzhelme in Zeiten zunehmender innerstaatlicher Gewalt**
Lothar H. Schuster

219 **Technologische Transformation und institutionelle Anpassung – Das Polizeitechnische Institut im digitalen Zeitalter**
Wilfried Honekamp

229 **Verzeichnis der Autorinnen und Autoren**

Strukturwandel der Polizeitechnik im 21. Jahrhundert – Entwicklungslinien und interdisziplinäre Perspektiven

Wilfried Honekamp und Gundula Gahlen

Polizeitechnik ist im 21. Jahrhundert nicht mehr als bloße Ausrüstung oder als nachgelagerte Unterstützung polizeilichen Handelns zu verstehen. Sie ist vielmehr als sozialer und organisationaler Faktor zu begreifen, der polizeiliche Handlungsmöglichkeiten mitstrukturiert (Nogala, 1995, S. 191–194). Des Weiteren prägt sie zunehmend die organisatorischen, rechtlichen, taktischen und professionellen Bedingungen, unter denen Polizei Sicherheit gewährleistet, Gefahren abwehrt, Straftaten verfolgt, Spuren sichert, kommuniziert und sich selbst schützt. Moderne Polizeitechnik reicht von persönlicher Schutzausstattung über Kommunikations- und Informationssysteme bis zu Einsatzfahrzeugen und Verkehrsüberwachungstechnik. Damit verschiebt sich der Blick: Nicht einzelne Geräte oder Systeme stehen isoliert im Zentrum, sondern die strukturellen Bedingungen, unter denen Technik polizeilich entwickelt, beschafft, reguliert, eingesetzt, bewertet und fortgeschrieben wird.

Dieser Band nimmt die Entwicklung aus unterschiedlichen fachlichen Perspektiven in den Blick. Er fragt nach den technischen Entwicklungslinien ebenso wie nach ihren rechtlichen, organisatorischen, kriminalistischen, forensischen, kommunikativen und ausbildungsbezogenen Voraussetzungen im historischen Wandel. Polizeitechnik erscheint dabei nicht als linearer Fortschrittsprozess, in dem neue technische Möglichkeiten ältere Verfahren lediglich ablösen. Vielmehr zeigt sich ein komplexes Wechselverhältnis zwischen Bedrohungslagen, Einsatzerfahrungen, rechtlichen Rahmungen, föderalen Entscheidungsstrukturen, wissenschaftlichem Erkenntnisfortschritt, industrieller Innovationsfähigkeit und polizeilicher Praxis. Ob und wie neue Technologien polizeilich genutzt werden, hängt dabei nicht nur vom fachlichen Bedarf ab. Ebenso entscheidend sind organisationsinterner Veränderungswille, politische und öffentliche Erwartungsdynamiken, haushalterische und personelle Ressourcen, technische Kompatibilität sowie die rechtlichen Grenzen von Technologien, die besonders stark in Grundrechte eingreifen können (Aden, 2025, S. 94–98). Auch die Ausgestaltung der Technik selbst wird durch Anforderungen aus Einsatzlagen, Verletzungs- und Gefährdungserfahrungen, Grundrechtsschutz, Standardisierung, Haushalts- und Beschaffungslogiken sowie institutionelles Wissen geprägt.

Ein zentrales Strukturmerkmal moderner Polizeitechnik liegt in ihrer Ambivalenz. Technik erweitert polizeiliche Handlungsfähigkeit. Sie kann Verfahren beschleunigen, Einsatzkräfte schützen, Ermittlungen präzisieren und neue kriminalistische Erkenntnisse ermöglichen. Zugleich erzeugt sie neue Risiken und hängt von organisatorischen und nutzungsbezogenen Bedingungen ab (Koper et al., 2015, S. 4–5). Automatisierte Datenanalysen können Zusammenhänge sichtbar machen, die manuell nicht erkennbar wären. Sie können aber auch Eingriffstiefen erzeugen, die rechtlich eigenständig zu bewerten sind. Digitale Forensik ermöglicht die Sicherung und Auswertung flüchtiger, verteilter und verschlüsselter Spuren. Sie ist jedoch auf belastbare Methoden, Dokumentationsstandards und gerichtsfeste Nachvollziehbarkeit angewiesen. Kommunikationsplattformen und Social Media eröffnen neue Formen polizeilicher Öffentlichkeitsarbeit, erhöhen aber zugleich die Anforderungen an strategische

Kommunikation, Medienkompetenz und institutionelle Reaktionsfähigkeit. Schutzausstattung kann Leben und Gesundheit von Einsatzkräften sichern, muss jedoch technisch und ergonomisch so ausgestaltet sein, dass sie im Einsatz tatsächlich beherrschbar bleibt.

Gerade weil Polizeitechnik so vielfältige technische, rechtliche, kommunikative und organisatorische Fragen aufwirft, muss sie interdisziplinär betrachtet werden. Ihre Entwicklung lässt sich weder allein aus der Ingenieurwissenschaft noch allein aus der Rechtswissenschaft, Kriminalistik, Informatik, Organisationsforschung oder Kommunikationswissenschaft erklären. Rechtliche, ethische und sozialwissenschaftliche Perspektiven sollten bereits bei der Entwicklung und Bewertung technischer Lösungen einbezogen werden (Aden et al., 2023, S. 285–286).

Rechtliche Anforderungen an automatisierte und KI-gestützte Datenverarbeitung ergeben sich aus dem Zusammenspiel von Datenschutzrecht, Verfassungsrecht, europäischer Regulierung und technischer Systemarchitektur. Digitale Forensik bewegt sich zwischen Informatik, Kriminalistik, Beweisrecht und methodischer Qualitätssicherung. Polizeiliche Datenplattformen betreffen nicht nur IT-Architekturen, sondern auch die Datenqualität, Interoperabilität, organisatorische Zuständigkeiten und die Einbindung datenanalytischer Expertise in polizeiliche Arbeitsprozesse. Datengetriebene Polizeiarbeit führt unterschiedliche Datenquellen mit analytischen Verfahren und operativen Folgemaßnahmen zusammen. Ihre Wirkung hängt deshalb von institutionellen Rahmenbedingungen, organisationaler Einbettung und den Datenkompetenzen der beteiligten Akteurinnen und Akteure ab (Afzal & Panagiotopoulos, 2025, S. 411–413, 417–422). Cybercrime wiederum verdeutlicht, dass Kriminalitätsformen, Ermittlungsinstrumente und technologische Infrastrukturen nicht getrennt betrachtet werden können. Auch technische Richtlinien für Einsatzhelme zeigen exemplarisch, wie Materialkunde, Ballistik, Prüfverfahren, Einsatztaktik und Erfahrungswissen ineinandergreifen.

Die Interdisziplinarität moderner Polizeitechnik ist keine bloß theoretische Anforderung, sondern eine praktische Notwendigkeit. Polizeiliche Technikentscheidungen entfalten weitreichende Folgen für Ausbildung, Einsatzorganisation und Beschaffung sowie für Führungsprozesse und Dokumentation. Zugleich beeinflussen sie den Grundrechtsschutz, die Fehlerkultur und die öffentliche Legitimation polizeilichen Handelns. Wer neue Technik einführt, verändert Arbeitsweisen. Dies gilt insbesondere dort, wo neue Technik die Wahrnehmung, Priorisierung, Bewertung oder Entscheidungsvorbereitung beeinflusst. Die Wirkung solcher Systeme hängt maßgeblich vom Zusammenspiel mit polizeilichen Routinen, Führungspraktiken, der Organisationskultur und der Akzeptanz durch die Nutzenden ab (Koper et al., 2015, S. 3–5). Die Frage, ob Technik die Menschen entlastet oder schrittweise zum bloßen Bediener systemischer Vorgaben macht, betrifft den professionellen Kern polizeilicher Arbeit in einem demokratischen Rechtsstaat. Gerade datengetriebene Verfahren verschieben das Verhältnis von Erfahrung und professioneller Ermessensausübung, ohne menschliche Kontextbewertung vollständig ersetzen zu können (Afzal & Panagiotopoulos, 2025, S. 422–424).

Ein weiteres Strukturmerkmal liegt in der Beschleunigung technologischer Entwicklung. Während frühere technische Innovationen vor ihrer Einführung häufig über längere Zeiträume entwickelt, erprobt und standardisiert wurden, entstehen heutige Innovationszyklen in deutlich kürzeren Abständen. Digitale Kommunikationsformen, mobile Endgeräte, KI-Anwendungen, Cloud-Dienste, vernetzte Fahrzeuge, private Plattformökonomien und globale Cybercrime-

Infrastrukturen verändern auch die Erwartung an polizeiliche Reaktionsgeschwindigkeit. Polizeien müssen Technologien verstehen, bevor ihr Missbrauch zu massenhaften Phänomenen wird. Zugleich dürfen sie sich nicht von bloßer Innovationsrhetorik treiben lassen. Gerade im Sicherheitsbereich ist die Frage entscheidend, ob eine Technik einsatztaktisch erforderlich, rechtlich tragfähig, organisatorisch beherrschbar, methodisch valide und gesellschaftlich legitimierbar ist. Bei datengetriebenen und algorithmisch vermittelten Verfahren schließt dies ein, dass Datenflüsse kontrollierbar bleiben, Abhängigkeiten von externen Anbietern begrenzt werden, analytische Prozesse nachvollziehbar sind und polizeiliches Handeln gegenüber der Öffentlichkeit rechenschaftsfähig bleibt (Leese, 2024, S. 963–966, 971–973).

Die Entwicklung moderner Polizeitechnik ist außerdem eng mit Wissensmanagement verbunden. Viele technische Fortschritte entstehen durch das Zusammenwirken besonders erfahrener Personen, spezialisierter Einheiten und wissenschaftlicher Expertise sowie durch die Einbindung von Prüfstellen, Herstellern und Anwendern. Gerade bei digitalen Spuren und cyberbezogenen Phänomenen müssen Erkenntnisse über neue Technologien, mögliche Dual-Use-Potenziale und kriminalistische Relevanz frühzeitig in Aus- und Fortbildung, Prävention und Ermittlungsverfahren überführt werden (Honekamp et al., 2023, S. 688–689, 695–696). In der Praxis ist dieses Wissen allerdings häufig implizit und erfahrungsgebunden. Geht es verloren, können technische Richtlinien und Einsatzmittel zwar fortbestehen, ohne dass ihr Entwicklungsprozess hinreichend verstanden wird. Gerade in hochspezialisierten Bereichen wie Schutzausstattung, Einsatzfahrzeugtechnik, Verkehrsüberwachung oder Informations- und Kommunikationstechnik ist aber die kontinuierliche Fähigkeit der Polizei, Technik kompetent und kritisch zu bewerten, entscheidend.

Die Beiträge in diesem Band verdeutlichen damit, dass Polizeitechnik immer auch Ausdruck institutioneller Anpassung ist. Sie reagiert auf veränderte Bedrohungslagen, neue Kriminalitätsformen, gesellschaftliche Kommunikationsgewohnheiten und rechtliche Anforderungen. Gleichzeitig verändert sie die Polizei selbst, indem sie beeinflusst, wie Einsatzlagen wahrgenommen, Informationen verteilt, Spuren interpretiert, Risiken bewertet und Entscheidungen vorbereitet werden. Technik ist damit nicht neutral im Sinne bloßer Zweckmäßigkeit. Sie strukturiert Möglichkeiten, setzt Prioritäten, erzeugt Routinen und wirkt als Verstärker polizeilicher Handlungs- und Kontrollmacht, die in demokratischen Rechtsstaaten legitimiert und kontrolliert werden muss (Leese, 2024, S. 965–966, 973–974; Nogala, 1995, S. 193–194, 206–207). Die Beiträge zeigen aus unterschiedlichen Perspektiven, dass sich die Entwicklung der Polizeitechnik im 21. Jahrhundert im Spannungsfeld von Innovation und Kontrolle, Schutz und Eingriff, Effizienz und Rechtsstaatlichkeit, Spezialisierung und Alltagspraxis sowie föderaler Vielfalt und dem Bedarf an gemeinsamen Standards vollzieht. Gerade hierin liegen die Strukturbedingungen moderner Polizeitechnik.

Dirk Kunze analysiert die europa- und verfassungsrechtlichen Anforderungen an die polizeiliche Datenverarbeitung beim Einsatz automatisierter und KI-gestützter Systeme. Im Zentrum stehen das Mehrebenensystem aus Grundgesetz, Grundrechtecharta und EMRK, die Abgrenzung von DSGVO, JI-Richtlinie und AI Act. Darüber hinaus untersucht der Beitrag die verfassungsrechtliche Bewertung automatisierter Datenanalysen, biometrischer Daten, KI-gestützter Priorisierung und OSINT-Verknüpfungen. Der Beitrag zeigt, dass automatisierte und KI-gestützte Verfahren nicht lediglich effizientere Formen herkömmlicher Datenverar-

beitung darstellen. Aufgrund ihrer besonderen Eingriffstiefe erfordern sie vielmehr eigenständige gesetzliche Grundlagen sowie differenzierte Eingriffsschwellen. Ebenso bedürfen sie Zweckbindungen sowie Transparenz-, Dokumentations- und Kontrollmechanismen.

Die Entwicklung der polizeilichen Presse- und Öffentlichkeitsarbeit steht im Mittelpunkt des Beitrags von Stefan Jarolimek. Ausgehend von frühen Pressestellen und klassischen Kommunikationsmitteln wie Telefon, Brief und Fax beschreibt er den Wandel hin zu Internet, Intranet, Social Media, crossmedialem Kommunikationsmanagement und neuen Plattformlogiken. Er zeigt, dass sich polizeiliche Öffentlichkeitsarbeit nicht nur technisch erweitert, sondern auch organisatorisch professionalisiert und strategisch ausdifferenziert hat. Aktuelle Entwicklungen wie Twitch und der Einsatz von KI in der Kommunikation verdeutlichen, dass polizeiliche Kommunikationsarbeit heute eigene technische Infrastrukturen, spezialisierte Kompetenzen sowie medienrechtliche und ethische Reflexion benötigt.

Dirk Labudde und Roman Povalej verbinden die kriminalistische Systematik Ernst Gennats aus der Weimarer Republik mit den Anforderungen digitaler Forensik. Der Beitrag rekonstruiert Gennats methodisches Denken als praxisbasierte und hypothesengeleitete Erkenntnisordnung, deren methodische Grundgedanken bis heute institutionell nachwirken. Er überträgt diesen Ansatz auf digitale Spuren, mobile Forensik, das Cybermobil, Dual-Use-Technologien und kriminalistische Innovationszyklen. Damit wird der historische Bezug nicht nostalgisch verwendet, sondern als methodischer Maßstab für digitale Ermittlungsumgebungen fruchtbar gemacht. Der Beitrag zeigt, dass moderne Forensik nicht allein durch neue Werkzeuge entsteht, sondern durch die Fähigkeit, technische Möglichkeiten in eine kontrollierte kriminalistische Erkenntnismethodik einzubetten.

Die Entwicklung der Automatisierung bei der Polizei – von der Rasterfahndung über POLAS-Sammelabfragen bis hin zum Einsatz Künstlicher Intelligenz – bildet den Schwerpunkt des Beitrags von Andreas Beier. Er verbindet polizeihistorische Entwicklungslinien mit der Frage, wie technische Systeme das Berufsbild, die Wahrnehmung und die Handlungsspielräume von Polizistinnen und Polizisten verändern. Dabei geht es nicht nur um Effizienzgewinne, sondern auch um die Gefahr, dass polizeiliche Erfahrung, Empathie, Intuition und berufsethische Urteilskraft durch automatisierte Vorgaben überlagert werden. Die zugespitzte Frage nach dem „Technikbeiwerk“ markiert deshalb eine zentrale professionelle Spannung moderner Polizeiarbeit.

Anosch Amanat untersucht die Entwicklung polizeilicher Datenarchitekturen seit 2000 von fachlich begrenzten Insellösungen über Integrationsansätze hin zu Datenplattformen. Der Beitrag arbeitet heraus, dass polizeiliche Datenverarbeitung nicht länger nur einzelne Arbeitsabläufe unterstützt, sondern mittlerweile die infrastrukturelle Grundlage für Ermittlungen, Lagebilder, Führungsentscheidungen und perspektivisch automatisierte Analysen geworden ist. Im Zentrum steht damit nicht nur die technische Modernisierung von IT-Systemen, sondern eine Veränderung der polizeilichen Informationsordnung. Damit rücken Fragen der Datenqualität, Interoperabilität, Zugriffsregelung, Zweckbindung und organisatorischen Zuständigkeit in den Mittelpunkt.

Der Beitrag von Andreas Mehlich und Kilian L. Scholz zeichnet nach, wie digitale Fahrzeugdaten im 21. Jahrhundert zu einem wichtigen Bestandteil moderner Polizeitechnik geworden sind. Die Autoren zeigen, wie sich das Kraftfahrzeug vom mechanischen Fortbewegungsmittel zu einem vernetzten, datengestützten System entwickelt hat. Dadurch entstehen neue Spurenquellen für Verkehrsunfallaufnahme, Unfallrekonstruktion und Ermittlungsverfahren. Zugleich wird herausgearbeitet, dass dieses Potenzial in der polizeilichen Praxis bislang nur punktuell ausgeschöpft wird und standardisierte Verfahren, technische Ausstattung sowie rechtliche Sensibilisierung weiterentwickelt werden müssen. Die Car-Forensik erweist sich damit als Beispiel für ein Feld, in dem technische Datenverfügbarkeit erst durch rechtlich und methodisch abgesicherte Verfahren polizeilich nutzbar wird.

Heiko Rittelmeier zeichnet die Entwicklung der digitalen Forensik von physischen Datenträgern bis zur Cloud nach. Der Beitrag beschreibt digitale Beweismittel als inzwischen nahezu deliktsübergreifend relevante Informationsquellen und ordnet die digitale Forensik als Schnittfeld von Informatik, Strafprozessrecht und kriminaltechnischer Methodik ein. Neben den Pionierjahren und der Professionalisierung der Disziplin werden aktuelle Herausforderungen durch Cloud-Dienste, IoT-Geräte, verteilte Datenbestände, proprietäre Systeme und internationale Zuständigkeiten herausgearbeitet. Dabei wird besonders deutlich, dass digitale Forensik auf Standardisierung, Nachvollziehbarkeit und institutionelle Forschung angewiesen ist, um digitale Beweise gerichtsfest sichern und auswerten zu können.

Der Beitrag von Dirk Labudde zeichnet die Entwicklung der Tatortdokumentation von zweidimensionaler Fotografie und Skizzen über digitale Modellierung, 3D-Erfassung, Photogrammetrie, Laserscanning und immersive Technologien bis hin zum digitalen Zwilling in der Forensik nach. Der digitale Zwilling ist ein maßstabsgetreues, dauerhaft nutzbares digitales Abbild realer Tatorte oder Objekte. Er wird dabei nicht nur als Visualisierungsinstrument verstanden, sondern als Bestandteil eines hypothesengeleiteten forensischen Erkenntnissystems. Zugleich weist der Beitrag auf die normativen Anforderungen an Datenintegrität, Dokumentation, Nachvollziehbarkeit und gerichtliche Präsentation hin, weil digitale Modelle auch suggestive Wirkungen entfalten können.

Robert Diedrich Ulrich Lippitz untersucht digitale Fälschungen von einfachen Bildmanipulationen bis hin zu Deepfakes. Der Beitrag zeigt zunächst, dass visuelle Fälschungen keine Erfindung des digitalen Zeitalters sind. Durch digitale Werkzeuge und Künstliche Intelligenz haben ihre Herstellung und Verbreitung jedoch eine neue Qualität erreicht. Deepfakes werden als Angriffe auf die Vertrauensinfrastruktur moderner Gesellschaften eingeordnet. Für Polizei und Forensik ergibt sich daraus eine doppelte Aufgabe: Einerseits müssen Manipulationen technisch besser erkannt werden, andererseits sind Verfahren zu entwickeln, die Herkunft, Überlieferung und Beweiswert digitaler Evidenz belastbar absichern.

Die Entwicklung von Computerkriminalität zu Cybercrime im 21. Jahrhundert beschreibt Wilfried Honekamp. Er zeichnet anhand polizeilicher Veröffentlichungen, insbesondere der Polizeilichen Kriminalstatistik und der Bundeslagebilder Cybercrime, den Wandel von technisch geprägten Einzeldelikten hin zu arbeitsteiligen, transnational vernetzten und ökonomisierten Kriminalitätsmodellen nach. Cybercrime wird dabei als Querschnittsbedrohung sichtbar, die polizeiliche Ermittlungsinstrumente, forensische Informatik, Prävention, inter-

nationale Kooperation und Datenanalyse gleichermaßen betrifft. Der Beitrag verdeutlicht, dass Kriminalitätsformen, technische Infrastrukturen und die Entwicklung polizeilicher Technik wechselseitig aufeinander bezogen sind.

Johannes Fähndrich und Wilfried Honekamp richten den Blick auf die polizeiliche Ausbildung als notwendige Bedingung technischer Handlungsfähigkeit. Der Beitrag argumentiert, dass die Entwicklung der Polizeitechnik nicht allein eine Frage von Beschaffung, Ausstattung oder operativer Anwendung ist, sondern eine parallele Weiterentwicklung von Ausbildung, curricularer Steuerung und institutioneller Wissensverarbeitung erfordert. Am Beispiel der Hochschule für Polizei Baden-Württemberg als exemplarischem Bezugspunkt wird die Gefahr einer technologischen Entkopplung sichtbar: Während digitale und KI-gestützte Technologien zunehmend polizeiliche Praxis prägen, folgen Studienordnungen, Lehrformate und institutionelle Transferstrukturen häufig langsameren Anpassungslogiken. Technik wird unter diesen Bedingungen nicht automatisch zum Gewinn. Ihr Nutzen hängt vielmehr davon ab, ob Polizeihochschulen technische Entwicklungen frühzeitig beobachten, rechtlich und methodisch einordnen und in belastbare Ausbildungsinhalte überführen können.

Lothar H. Schuster untersucht die Bedeutung technischer Richtlinien für Einsatzhelme in Zeiten zunehmender innerstaatlicher Gewalt. Er beschreibt die Entwicklung des Kopfschutzes für Bereitschaftspolizeien und Spezialeinsatzkommandos und zeigt, wie Einsatzerfahrungen, Erkenntnisse aus der Materialkunde, Prüfverfahren und Standardisierungsprozesse in die Entwicklung neuer Schutzkonzepte einfließen. Besonders deutlich wird, dass technische Richtlinien nicht bloße Beschaffungsdokumente sind, sondern verdichtetes Erfahrungswissen zu Gefährdungslagen, Schutzbedarfen und einsatztaktischen Anforderungen enthalten. Der Beitrag macht zugleich sichtbar, wie verletzlich solches Wissen ist, wenn es nicht institutionell gesichert, fortgeschrieben und zwischen Polizei, Prüfstellen und Herstellern kontinuierlich ausgetauscht wird.

Wilfried Honekamp widmet sich abschließend der technologischen Transformation und institutionellen Anpassung des Polizeitechnischen Instituts im digitalen Zeitalter. Der Beitrag rekonstruiert die Entwicklung des PTI von der früheren Forschungs- und Entwicklungsstelle für Polizeitechnik hin zu einer fachtechnischen Koordinierungs-, Beratungs-, Wissens- und Transferinstanz. Mit der Digitalisierung verschiebt sich der institutionelle Bedarf von der Prüfung einzelner Produkte hin zur Bewertung komplexer soziotechnischer Systeme, einschließlich Datenverarbeitung, Interoperabilität, KI, mobiler Endgeräte, Sensorik und Technologiefrüherkennung. Das PTI steht damit beispielhaft für die institutionellen Herausforderungen moderner Polizeitechnik: Technologische Entwicklungen müssen frühzeitig erkannt, fachlich bewertet, rechtlich und organisatorisch eingeordnet und in die polizeiliche Praxis zurückgekoppelt werden.

Insgesamt lässt der historische Blick auf die Polizeitechnik im 21. Jahrhundert einen tiefgreifenden Strukturwandel erkennen. Während technische Innovationen früher vielfach einzelne Einsatzmittel oder Arbeitsabläufe betrafen, prägen heute Digitalisierung, datengetriebene Verfahren und Künstliche Intelligenz ganze Informations- und Entscheidungsprozesse. Datenplattformen, digitale Forensik, vernetzte Kommunikationsstrukturen und die Bekämpfung von Cybercrime zeigen, dass Polizeitechnik zunehmend als komplexes Zusammenspiel technischer, organisatorischer und rechtlicher Systeme verstanden werden muss.

Zugleich verdeutlichen die Beiträge, dass der erfolgreiche Einsatz moderner Polizeitechnik von den Einsatzanforderungen, den rechtlichen Rahmenbedingungen, der Standardisierung, den Dateninfrastrukturen, der forensischen Methodik sowie von organisationaler Lernfähigkeit und professioneller Ausbildung abhängt. Technische Entwicklung in der Polizei ist nur dann tragfähig, wenn sie mit Rechtsstaatlichkeit, methodischer Qualität, institutionellem Wissensmanagement und praktischer Handlungskompetenz verbunden bleibt.

Referenzen

Aden, H. (2025). Die polizeiliche Nutzung neuer Technologien zwischen Wollen, Sollen, Können und Dürfen. In A. Dessecker & M. Rettenberger (Hrsg.), Die Zukunft der Kriminalität und ihrer Kontrolle (S. 91–102). Kriminologische Zentralstelle. https://www.krimz.de/fileadmin/dateiablage/E-Publikationen/KuP-Online/KuP-online1.pdf

Aden, H., Fährmann, J., & Matzdorf, C. (2023). Technikforschung und Polizei – strukturelle Rahmenbedingungen, Hindernisse und Perspektiven. In J. Fährmann, G. Görlitz, C. Matzdorf & A. Vollmar (Hrsg.), Private Positionsdaten und polizeiliche Aufklärung von Diebstählen: Rechtliche, kriminalistische und technische Perspektiven (S. 279–289). Nomos. https://doi.org/10.5771/9783748900320-279

Afzal, M., & Panagiotopoulos, P. (2025). Data in policing: An integrative review. International Journal of Public Administration, 48(7), 411–430. https://doi.org/10.1080/01900692.2024.2360586

Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., & Labudde, D. (2023). Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2. Phänomene und Auswirkungen (S. 673–702). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_51

Koper, C. S., Lum, C., Willis, J. J., Woods, D. J., & Hibdon, J. (2015). Realizing the potential of technology in policing: A multisite study of the social, organizational, and behavioral aspects of implementing policing technologies. National Institute of Justice. https://nij.ojp.gov/library/publications/realizing-potential-technology-policing-multisite-study-social-organizational

Leese, M. (2024). Staying in control of technology: Predictive policing, democracy, and digital sovereignty. Democratization, 31(5), 963–978. https://doi.org/10.1080/13510347.2023.2197217

Nogala, D. (1995). The future role of technology in policing. In J.-P. Brodeur (Hrsg.), Comparisons in policing: An international perspective (S. 191–210). Avebury. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-74150-8

Europa- und verfassungsrechtliche Anforderungen an die polizeiliche Datenverarbeitung beim Einsatz automatisierter und KI-gestützter Systeme

Dirk Kunze

Die polizeiliche Datenverarbeitung befindet sich im Zuge der Digitalisierung in einem tiefgreifenden Wandel: Automatisierte Analysesysteme, Data-Mining-Verfahren und zunehmend auch KI-gestützte Anwendungen versprechen Effizienzgewinne und eine bessere Bewältigung komplexer Gefahrenlagen, erhöhen aber zugleich das grundrechtliche Risiko für Betroffene. Technische Entwicklungen wie die Auswertung von Bildern und Videos, biometrische Identifikation, OSINT-basierte Profile oder prädiktive Analysen verschärfen die Eingriffstiefe und verändern qualitativ die Art des Eingriffs in Freiheitsrechte.

Nachfolgend sollen die europa- und verfassungsrechtlichen Anforderungen an die polizeiliche Datenverarbeitung unter besonderer Berücksichtigung automatisierter und KI-Systeme systematisch dargestellt werden. Im Mittelpunkt stehen die Eingriffsschwellen und die Eingriffstiefe, die Anforderungen an Ermächtigungsgrundlagen, die rechtliche Einordnung von Bildern und Videos als personenbezogene Daten, die Problematik KI-gestützter Priorisierung ohne eigene gesetzliche Grundlage sowie die Verknüpfung offen zugänglicher Informationen (OSINF/OSINT (Ackerschott, S. 40−42)) mit polizeilichen Datenbeständen. OSINF (Open Source Information) bezeichnet dabei die bloßen Informationen, während OSINT (Open Source Intelligence) bereits eine Kontextualisierung, Verdichtung und Bewertung dieser Informationen umfasst (Ackerschott, S. 40 ff.).

Mehrebenensystem des Grundrechtsschutzes – EMRK, GRC und Grundgesetz

Die Bewertung der Grundrechtsrelevanz polizeilicher Datenverarbeitung im Kontext automatisierter und KI-gestützter Verfahren erfolgt in einem europäischen Mehrebenensystem aus Europäischer Menschenrechtskonvention (EMRK), Grundrechtecharta (GRC) und Grundgesetz. Die EMRK wirkt als völkerrechtlicher Vertrag über Art. 59 Abs. 2 GG in die nationale Rechtsordnung hinein und ist durch den Europäischen Gerichtshof für Menschenrechte (EGMR) nur subsidiär kontrolliert. Primär sind die Vertragsstaaten für die Gewährleistung der Rechte verantwortlich und müssen einen effektiven Grundrechtsschutz sicherstellen (*Van Gend en Loos v Administratie der Belastingen,* 05.02.1963).

Die GRC ist demgegenüber originäres Unionsrecht und bindet die Mitgliedstaaten, soweit sie Unionsrecht durchführen (Art. 51 GRC). Der Gerichtshof der Europäischen Union (EuGH) hat den Anwendungsvorrang des Unionsrechts betont: Nationale Rechtsnormen – auch verfassungsrechtliche – treten im Kollisionsfall im Anwendungsbereich des Unionsrechts zurück, ohne dass ihr Geltungsanspruch als solcher aufgehoben würde (Anwendungsvorrang, kein Geltungsvorrang). Damit bestimmt sich der Prüfungsmaßstab für polizeiliche Datenverarbeitung im Anwendungsbereich unionsrechtlicher Vorgaben primär nach der GRC.

Das Bundesverfassungsgericht (BVerfG) hat mit den „Solange“-Entscheidungen und dem Maastricht-Beschluss ein kooperatives Verhältnis zum EuGH entwickelt. Solange die Union einen im Wesentlichen gleichwertigen Grundrechtsschutz gewährleistet, übt das BVerfG eine zurückgenommene Kontrolle aus, die auf die Wahrung unabdingbarer Grundrechtsstandards und die Sicherung der Verfassungsidentität gerichtet ist (Art. 79 Abs. 3 GG, Art. 4 Abs. 2 EUV). Nur wenn diese Grenzen überschritten werden, kommt eine eigenständige verfassungsgerichtliche Korrektur in Betracht (*Solange I,* 29.05.1974; *Solange II,* 22.10.1986).

Determiniertes und nicht determiniertes Unionsrecht

Für die polizeiliche Datenverarbeitung ist entscheidend, ob in einem Regelungsbereich vollständig unionsrechtlich determiniertes Recht vorliegt oder ob nationale Gestaltungsspielräume verbleiben. Ist ein Sachbereich – wie etwa die privatrechtliche Datenverarbeitung nach der Datenschutz-Grundverordnung (DSGVO) – weitgehend durch unmittelbar anwendbares Unionsrecht determiniert, richtet sich die Grundrechtsprüfung primär nach der GRC und der Auslegung durch den EuGH. Nationale Grundrechte treten insoweit als eigenständiger Prüfungsmaßstab zurück, soweit nicht die Verfassungsidentität berührt ist.

Verbleiben hingegen Spielräume – wie bei der Richtlinie (EU) 2016/680 (JI-Richtlinie) – kommt neben der GRC weiterhin das nationale Grundrechtsregime zur Anwendung. Die Richtlinie setzt Mindeststandards, überlässt den Mitgliedstaaten jedoch die Ausgestaltung vieler Detailfragen. In diesen „offenen“ Bereichen kann und muss das Grundgesetz ein eigenes Schutzniveau sicherstellen, etwa durch das Bestimmen von Eingriffsschwellen, differenziertere Zweckbindungen oder weitergehende Transparenz- und Kontrollpflichten (JI-Richtlinie, 2016/04.05.2016).

Nach Art. 53 GRC ist dabei stets das jeweils „meistbegünstigende“ Schutzniveau maßgeblich: Gewährt das Grundgesetz einen weitergehenden Schutz als die GRC, ist dieser weitergehende Schutz im Rahmen der nationalen Spielräume zu beachten. Das führt im Bereich der polizeilichen Datenverarbeitung dazu, dass die verfassungsgerichtlichen Leitlinien zur informationellen Selbstbestimmung neben den unionsrechtlichen Vorgaben weiterhin eine eigenständige Rolle spielen (Kunze, 2026, S. 1447).

Europarechtlicher Rahmen: DSGVO, JI-Richtlinie und AI Act

<u>Abgrenzung von DSGVO und JI-Richtlinie</u>

Die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) regelt die Verarbeitung personenbezogener Daten im allgemeinen Bereich, insbesondere durch private Verantwortliche und öffentliche Stellen außerhalb von Strafverfolgung und Gefahrenabwehr. Nach Art. 2 Abs. 2 lit. d und e DSGVO ist sie jedoch nicht auf Verarbeitungen durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie zur Abwehr von Gefahren für die öffentliche Sicherheit anwendbar. Diese fallen in den Anwendungsbereich der JI-Richtlinie (DSGVO, 2016).

Art. 1 Abs. 1 JI-Richtlinie erfasst alle Verarbeitungen personenbezogener Daten durch zuständige Behörden zum Zwecke der Strafverfolgung, Verhütung und Aufdeckung von Straftaten sowie des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, unabhängig davon, ob sie automatisiert oder nicht automatisiert erfolgen. Sie richtet sich damit unmittelbar an Polizei- und Strafverfolgungsbehörden. Die Richtlinie setzt Mindeststandards, lässt den Mitgliedstaaten aber ausdrücklich Spielräume für strengere Regelungen. Sie ist mithin kein vollständig determiniertes Unionsrecht (JI-Richtlinie, 2016/04.05.2016).

Im nationalen Recht – etwa im Bundesdatenschutzgesetz (BDSG) oder im Datenschutzgesetz NRW (DSG NRW) – werden die Begriffe der JI-Richtlinie weitgehend wortgleich übernommen. So definieren Art. 3 Nr. 1 JI-Richtlinie und § 36 Nr. 1 DSG NRW personenbezogene Daten als alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Hierzu zählen ausdrücklich auch Online-Kennungen, Pseudonyme und sonstige Merkmale der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität. Dabei orientiert sich die Frage, ob eine Information zur Identifizierbarkeit führt oder nicht, nicht an allgemeinen oder übergreifenden Aspekten, sondern konkret am Verarbeiter der Daten und Informationen, an den dortigen technischen Möglichkeiten und am Organisationswissen (Kunze, 2026, S. 1463 f.).

AI Act als risikobasierter Technikrahmen

Mit der Verordnung (EU) 2024/1689 (AI Act) schafft die Union einen sektorübergreifenden, risikobasierten Rechtsrahmen für Entwicklung, Inverkehrbringen und Nutzung von KI-Systemen im Binnenmarkt. Zweck der Verordnung ist es, „menschenzentrierte und vertrauenswürdige“ KI zu fördern und zugleich ein hohes Niveau des Schutzes von Gesundheit, Sicherheit und Grundrechten sicherzustellen. Der Fokus liegt nicht auf einzelnen Sektoren, sondern auf den Risiken, die aus dem Einsatz von KI-Systemen in unterschiedlichsten Anwendungsfeldern resultieren (EU AI Act, 2024).

Der AI Act unterscheidet verbotene KI-Systeme (nicht akzeptables Risiko), Hochrisiko-Systeme mit strengen Pflichten (u. a. Risikomanagement, Datenqualität, Transparenz, menschliche Aufsicht) und Systeme mit geringem oder begrenztem Risiko, für die vor allem Transparenzanforderungen gelten. Zugleich stellt der Gesetzgeber klar, dass die Verordnung selbst keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten schafft. Fragen der Zulässigkeit der Datenverarbeitung verbleiben im Anwendungsbereich der DSGVO und der JI-Richtlinie.

Besondere Bedeutung hat die enge Definition nationaler Sicherheit: Art. 2 Abs. 3 AI Act und die Erwägungsgründe stellen klar, dass Maßnahmen der nationalen Sicherheit nicht in die Zuständigkeit der Union fallen (Art. 4 Abs. 2 EUV) (Kunze, 2026, S. 1441). KI-Systeme, die für militärische oder genuin nationale Sicherheitszwecke entwickelt und ausschließlich in diesem Rahmen verwendet werden, sind daher vom Anwendungsbereich ausgenommen; werden sie für zivil-polizeiliche Zwecke eingesetzt, gilt der AI Act. So entsteht ein Spannungsfeld: Einerseits bleiben Straf- und Polizeirecht als „Wesenskern“ staatlicher Souveränität im

Kompetenzbereich der Mitgliedstaaten. Andererseits regelt der AI Act als Marktregulierung sehr weitgehend die Zulässigkeit bestimmter KI-Systeme auch für Zwecke der Strafverfolgung und Gefahrenabwehr.

KI-Systeme, biometrische Daten und biometrische Kategorisierung

Für die polizeiliche Datenverarbeitung zentral ist der KI-Systembegriff des AI Act: Nach Art. 3 umfasst er insbesondere maschinelle Lernverfahren, die mit einem bestimmten Grad an Autonomie aus Eingabedaten Ausgaben (Vorhersagen, Empfehlungen, Entscheidungen, Inhalte) erzeugen, welche physische oder virtuelle Umgebungen beeinflussen können. Dies schließt Systeme ein, die nach ihrer Einführung Anpassungsfähigkeit zeigen – also klassische Machine-Learning- und Deep-Learning-Ansätze –, und reicht damit über traditionelle, engere KI-Definitionen hinaus. Erfasst sind damit auch „schwache" KI-Systeme, die in der Praxis polizeilicher Datenverarbeitung häufig eingesetzt werden.

Erwägungsgrund 14 zum AI Act verweist ausdrücklich auf den Begriff der biometrischen Daten nach Art. 3 Nr. 13 JI-Richtlinie, der im Artikel 3 AI Act wortgleich übernommen wird. Zudem werden diese in Erwägungsgrund 15 u. a. um Gesicht, Augenbewegung, Körperform, Stimme, Gang oder Herzfrequenz erweitert, sofern diese eine Identifizierung ermöglichen. Für polizeiliche Systeme bedeutet dies, dass Bild- und Videodaten, die eine Identität erkennen oder biometrische Muster extrahieren lassen, regelmäßig als biometrische personenbezogene Daten zu qualifizieren sind. Sie unterfallen damit sowohl dem datenschutzrechtlichen Schutzregime als auch den verfassungsrechtlichen Anforderungen an besonders sensible Datenverarbeitungen.

Zudem normiert der AI Act den Begriff der „biometrischen Kategorisierung": Systeme, die Personen anhand biometrischer Merkmale in Kategorien mit bestimmten Eigenschaften, Risiken oder Verhaltensprofilen einordnen, werden – abhängig vom Zweck – teils als Hochrisiko-Systeme, teils sogar als verbotene Praktiken eingestuft. Dies betrifft insbesondere KI-gestützte Gesichtserkennung, Emotionserkennung oder Risikobewertungen im Polizeibereich, etwa bei Crowd-Management, Gefährderbewertung oder Zugangskontrollen.

Betroffene Grundrechte und Schutzdimensionen

Menschenwürde (Art. 1 Abs. 1 GG)

Die Menschenwürde nach Art. 1 Abs. 1 GG bildet das oberste Konstitutionsprinzip der Verfassungsordnung und zugleich den normativen Rahmen für alle weiteren Grundrechte. Sie schützt die Subjektqualität der Person, die Möglichkeit autonomer Selbstbestimmung und die Unverfügbarkeit des Menschen für staatliche Zwecke. Nach der bekannten Objektformel ist die Menschenwürde verletzt, wenn der Mensch zum bloßen Objekt staatlichen Handelns, zum bloßen Mittel oder zur „vertretbaren Größe" degradiert wird.

Für automatisierte und KI-gestützte Systeme bedeutet dies: Verfahren, die Personen vollständig standardisiert, ohne individuelle Betrachtung und ohne nachvollziehbare menschliche Kontrolle bewerten, klassifizieren oder über sie entscheiden, bergen ein erhebliches Risiko der Objektivierung. Besonders problematisch sind Konstellationen, in denen KI-Systeme Gefährlichkeitsaussagen oder Risikoprofile erzeugen, die trotz formaler menschlicher Entscheidung mangels Transparenz faktisch nicht überprüft werden können und Entscheidungsprozesse damit determinieren. Die Menschenwürdegarantie ist absolut und nicht abwägungsfähig. Eingriffe in ihren Kernbereich sind verfassungsrechtlich unzulässig – auch zur Abwehr schwerster Gefahren. Daraus folgt im Kontext polizeilicher Datenverarbeitung, dass bestimmte Formen umfassender Profilbildung, lückenloser Überwachung oder rein automatisierter Entscheidungsprozesse mit existenziellen Folgen von vornherein ausgeschlossen sind (*Automatisierte Datenanalyse,* 16.02.2023, RN 98).

Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wurde durch das Volkszählungsurteil 1983 als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) entwickelt. Es garantiert die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen, und schützt damit die Bedingungen für Privatheit, autonome Persönlichkeitsentfaltung und Verhaltensfreiheit (*Volkszählungsurteil,* 15.12.1983).

Zentrale Leitlinien der Rechtsprechung sind: Es gibt kein „belangloses Datum". Auch scheinbar triviale Informationen können in ihrer Aggregation grundrechtsrelevant werden. Das Risiko umfassender Persönlichkeitsprofile und Bewegungsbilder begründet ein besonderes Eingriffsgewicht. Dies gilt auch für Daten, die ursprünglich offen zugänglich waren oder durch die Datenbesitzer öffentlich gestellt wurden. Moderne Informationstechnik – einschließlich automatisierter und KI-gestützter Auswertungen – verschärft das Eingriffsgewicht qualitativ, weil sie die Grenzen menschlicher Bearbeitungsumfänge aufhebt, große Datenmengen dauerhaft verknüpfbar macht und neues Wissen generieren kann (*Automatisierte Kennzeichenerfassung,* 11.03.2008, RN 39).

Das BVerfG betont, dass die Gefährdung bereits darin liegt, dass personenbezogene Informationen in einer Weise genutzt und verknüpft werden können, die die Betroffenen weder überschauen noch beherrschen. Die tatsächliche Nutzung für belastende Maßnahmen ist keine Voraussetzung des Eingriffs. Schon die abstrakte Möglichkeit einer Auswertung in belastender Weise kann die Freiheitswahrnehmung nachhaltig beeinträchtigen (*Onlinedurchsuchung,* 2008, RN 198).

Weitere berührte Grundrechte

Neben Menschenwürde und informationeller Selbstbestimmung können durch polizeiliche Datenverarbeitung – insbesondere auch bei Social-Media-Monitoring, OSINT/OSINF und Profilbildung – weitere Grundrechte eröffnet werden:

- Gleichheit und Diskriminierungsverbot (Art. 3 GG),
- Religionsfreiheit (Art. 4 GG),
- Meinungsfreiheit (Art. 5 GG),
- Versammlungsfreiheit (Art. 8 GG),
- Vereinigungsfreiheit (Art. 9 GG),
- Fernmeldegeheimnis (Art. 10 GG) sowie die
- Unverletzlichkeit der Wohnung (Art. 13 GG).

Automatisierte Analyse von Daten, insbesondere Online-Kommunikation, Teilnahme an Versammlungen oder Gruppenzugehörigkeit kann Einschüchterungs- und Abschreckungseffekte („Chilling Effects“) entfalten und so die faktische Wahrnehmung dieser Rechte beeinträchtigen (*Journalistische Verbindungsdaten,* 12.3.2003, RN 98; *Rasterfahndung II,* 04.04.2006, RN 117).

Besonders im Fokus steht das Diskriminierungsverbot: KI-Systeme, die auf verzerrten Trainingsdaten oder problematischen Merkmalen (z. B. Ethnie, Religion, sozioökonomische Indikatoren) basieren, können mittelbare Benachteiligungen erzeugen. Das BVerfG verlangt, dass Ungleichbehandlungen nur auf hinreichend gewichtige Sachgründe gestützt und verfassungsrechtlich legitimiert werden dürfen. Die bloße statistische Korrelation genügt hierfür nicht (*Mediziner-BAföG,* 21.06.2011).

Eingriffskonzeption: Eingriffsstufen und Eingriffstiefe

Stufenmodell der Datenverarbeitung

Die Rechtsprechung des BVerfG differenziert innerhalb von Datenverarbeitungsvorgängen unterschiedliche Stufen, die jeweils eigenständige Eingriffe in das Recht auf informationelle Selbstbestimmung begründen:

- Erhebung personenbezogener Daten,
- erstmalige Speicherung personenbezogener Daten,
- weitere Speicherung und Aufbewahrung,
- Abfrage,
- Zugriff,
- interne Verwendung,
- Übermittlung,
- Verknüpfung mit anderen Beständen,
- Profilbildung sowie
- automatisierte Auswertung,
- Data-Mining und
- scoringbasierte Entscheidungen.

Je tiefer ein Datenverarbeitungsvorgang in die persönliche Lebensgestaltung eingreift, je heimlicher er erfolgt, je größer seine Streubreite ist, je stärker er neue, belastende Informationen generiert und je weiter die Betroffenen von der Gefahr oder der Straftat entfernt sind, zu deren Verhütung oder Bekämpfung der Eingriff erfolgt (Unbeteiligte, Kontaktperso-

nen), oder je höher das Risiko ist, dass die Betroffenen der Maßnahme Gegenstand weiterer Eingriffsmaßnahmen sind, ohne selbst die Ursache für die Datenverarbeitung gelegt zu haben, desto höher ist das Eingriffsgewicht und desto strenger sind die Anforderungen an die gesetzliche Ermächtigungsgrundlage (*Automatisierte Kennzeichenerfassung,* 11.03.2008, RN 69; *Bestandsdatenauskunft II,* 27.05.2020, RN 93; *Telekommunikationsüberwachung I,* 14.07.1999, RN 187 ff; *Zuordnung dynamischer IP-Adressen,* RN 123).

Streubreite, Heimlichkeit und Überwachungsgesamtrechnung

Maßnahmen mit großer Streubreite – etwa massenhafte Kennzeichenerfassung, flächendeckendes Scannen von Kommunikationsdaten oder automatisierte OSINT-Erhebungen – sind nicht deshalb milder, weil viele Personen betroffen sind. Vielmehr erhöht das verdachtslose Einbeziehen Unbeteiligter das Eingriffsgewicht. Die bloße Aufnahme in einen Datenverarbeitungszusammenhang erhöht das Risiko weiterer Auswertungen und Anschlussmaßnahmen („ins Visier geraten") (*Journalistische Verbindungsdaten,* 12.3.2003, S. 107; *Rasterfahndung II,* 04.04.2006, RN 82 f., 85; *Telekommunikationsüberwachung I,* 14.07.1999, RN 188).

Die Heimlichkeit einer Maßnahme wirkt ebenfalls eingriffsverschärfend: Betroffene können sich weder präventiv schützen noch nachträglich effektiv Rechtsschutz suchen. Benachrichtigungs- und Auskunftspflichten können diese strukturelle Asymmetrie nur teilweise kompensieren. Zudem weisen sie häufig Ausnahmen auf und werden, wenn überhaupt, nur retrograd wirksam. Mit dem Begriff der „Überwachungsgesamtrechnung" trägt das BVerfG dem Umstand Rechnung, dass zahlreiche, jeweils für sich genommen moderate Eingriffe in ihrer Summe zu einer qualitativ neuen Gefährdungslage führen können: Wenn über längere Zeit nahezu alle Bewegungen, Kontakte und Äußerungen einer Person registrierbar und auswertbar werden, droht eine faktische Rundumüberwachung, die die Menschenwürde tangieren kann (*BKAG, HyDane,* 20.04.2016, RN 82 m. w. N.).

Für automatisierte und KI-gestützte Verfahren ist die Überwachungsgesamtrechnung besonders bedeutsam, weil technische Systeme die bisherige Kapazitätsgrenze menschlicher Auswertung aufheben und Daten aus verschiedenen Quellen – inklusive OSINF/OSINT – leicht kombinierbar machen (*Automatisierte Datenanalyse,* 16.02.2023, RN 70).

Automatisierte Datenverarbeitung und Data-Mining

Automatisierte Datenverarbeitung stellt mehr als eine bloße Effizienzsteigerung gegenüber manuellen Verfahren dar. Systeme, die große, heterogene Datenbestände zusammenführen, normalisieren, analysieren bzw. statistisch auswertbar machen, erzeugen neues, grundrechtsrelevantes Wissen. Schon das Zusammenführen in eine auswertbare Struktur begründet ein eigenes Eingriffsgewicht.

Data-Mining-Verfahren – im Sinne der selbstständigen Suche nach Mustern, Zusammenhängen und Profilen – erhöhen die Eingriffstiefe eigenständig weiter. Sie können neue Verdachtsmomente und Handlungsanlässe generieren, die ohne diese Auswertung nicht entstanden wären, und sind deshalb nur in engen Grenzen zulässig. Das BVerfG verlangt für

derartige Methoden, insbesondere im polizeilichen Kontext, qualifizierte Eingriffsschwellen, klare Zweckbindungen und wirksame Kontrollmechanismen (*Automatisierte Datenanalyse,* 16.02.2023, RN 71 f.).

Anforderungen an Ermächtigungsgrundlagen

Bestimmtheit, Zweckbindung und Eingriffsschwellen

Polizeiliche Befugnisnormen, die in das Recht auf informationelle Selbstbestimmung eingreifen, müssen bereichsspezifisch, normenklar und präzise die Zwecke der Datenerhebung, die Art der Daten, die Methoden der Verarbeitung und die Nutzungsmöglichkeiten festlegen. Offene, weite oder „vagabundierende" Datensammlungen auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken sind verfassungsrechtlich unzulässig (*Automatisierte Kennzeichenerfassung,* 11.03.2008, RN 178).

Zentral ist die Zweckbindung: Daten dürfen grundsätzlich nur für den Zweck verarbeitet werden, zu dem sie erhoben wurden. Eine zweckändernde Nutzung stellt einen eigenständigen Eingriff dar und bedarf einer besonderen gesetzlichen Ermächtigung. Maßstab ist der Grundsatz der hypothetischen Datenneuerhebung: Die neue Nutzung ist nur zulässig, wenn die Daten für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln verfassungsrechtlich neu erhoben werden dürften. Die Eingriffsschwelle darf dabei niedriger liegen als bei der Erhebung selbst (*BKAG, HyDane,* 20.04.2016, LS 2).

Ermächtigungsgrundlagen haben darüber hinaus Eingriffsschwellen zu normieren, die sich am Gewicht des geschützten Rechtsgutes, am Gefahrengrad und an der Eingriffstiefe orientieren. Für besonders eingriffsintensive Maßnahmen – etwa heimliche Überwachungen, tiefgreifende Profilbildungen oder Zugriffe auf hochsensible Daten – verlangt das BVerfG regelmäßig eine zumindest „konkretisierte Gefahr" für besonders gewichtige Rechtsgüter (Leib, Leben, Freiheit der Person, Bestand oder Sicherheit von Bund und Ländern) (*Bestandsdatenauskunft II,* 27.05.2020, RN 149 m. w. N.).

Differenzierung nach Datenarten und Sensibilität

Je sensibler die Daten und je umfassender das entstehende Persönlichkeitsbild, desto höher die verfassungsrechtlichen Anforderungen. Daten, die die Biografie nachzeichnen, intime Lebensbereiche betreffen oder besondere Kategorien personenbezogener Daten (z. B. politische Überzeugungen, Religion, Gesundheitsdaten) enthalten, unterliegen strengeren Voraussetzungen. Aus unionsrechtlicher Sicht verstärken sich die Anforderungen weiter bei biometrischen Daten und bei Profiling im Sinne der DSGVO bzw. der JI-Richtlinie. Der AI Act führt für KI-Systeme, die mit solchen Daten arbeiten, einen zusätzlichen risikobezogenen Rechtsrahmen ein, ersetzt aber die materiellen Anforderungen an die Ermächtigungsgrundlagen nicht (Kunze, 2026, S. 1448 f.).

Automatisierte Entscheidungen und KI-gestützte Verfahren

Art. 22 DSGVO und Art. 11 JI-Richtlinie begrenzen automatisierte Entscheidungen, die rechtliche Wirkung entfalten oder Betroffene in ähnlicher Weise erheblich beeinträchtigen. Während die DSGVO belastende Entscheidungen grundsätzlich ausschließt, es sei denn, sie beruhen auf einer Rechtsnorm mit angemessenen Garantien, erlauben nationale Umsetzungen wie § 54 BDSG auch belastende Entscheidungen, wenn sie im Gesetz ausdrücklich vorgesehen sind (*Automatisierte Entscheidungsfindung – Begründung,* 12.09.2024).

Das BVerfG betrachtet rein automatisierte Entscheidungen, die ohne hinreichende menschliche Kontrolle zu Eingriffsakten führen, kritisch. Sie können mit der Menschenwürdegarantie kollidieren, wenn der Mensch letztlich zum Objekt undurchschaubarer Berechnungen gemacht wird. Aus diesem Grund werden automatisierte Entscheidungen bei belastenden Verwaltungsakten ausgeschlossen (*Automatisierte Datenanalyse,* 16.02.2023). KI-gestützte Systeme verstärken diese Problematik, weil ihre Entscheidungslogik – insbesondere bei selbstlernenden Modellen – oft nicht nachvollziehbar ist („Blackbox-Phänomen"). Dies bedeutet: Der Einsatz komplexer, insbesondere selbstlernender Verfahren erfordert eine eigenständige, hinreichend bestimmte gesetzliche Ermächtigungsgrundlage. Allgemeine Ermächtigungen zur automatisierten Datenverarbeitung genügen dem Bestimmtheitsgebot nicht, wenn sie leistungsfähige profilbildende oder KI-gestützte Systeme umfassen, ohne dabei Anlass, Datenbasis, Methoden, Zweckbindung, Schutzgüter, Eingriffsschwellen sowie Kontrollmechanismen differenziert zu regeln. Der Begriff Methoden schließt KI-Methoden ausdrücklich mit ein – diese sind durch den Gesetzgeber eigenständig zu normieren und können nicht unter allgemeine automatisierte Verfahren subsumiert werden (*Automatisierte Datenanalyse,* 16.02.2023, LS 4).

Bilder, Videos und biometrische Informationen als personenbezogene Daten

Persönliche Identifizierbarkeit durch Bild- und Videodaten

Nach Art. 3 Nr. 1 JI-Richtlinie und den korrespondierenden nationalen Datenschutzgesetzen sind personenbezogene Daten alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Eine Person gilt als identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu Kennungen oder besonderen Merkmalen, identifiziert werden kann. Entscheidend ist dabei nicht eine abstrakte allgemeine Identifizierbarkeit, sondern die Frage, ob die datenverarbeitende Stelle mit den ihr zur Verfügung stehenden Mitteln eine Person identifizieren kann.

Bilder und Videos, auf denen Personen erkennbar abgebildet sind, enthalten eine Vielzahl solcher Merkmale: Gesichtszüge, Körperstatur, Gangbild, Tätowierungen, Kleidung, kontextbezogene Informationen (Ort, Zeit, anwesende Personen) und ggf. Metadaten. Bereits ohne spezielle Technik können Betrachter aus diesen Daten Rückschlüsse auf Identität, Verhalten, soziale Zugehörigkeit oder politische Einstellungen ziehen.

Werden Bild- und Videodaten algorithmisch verarbeitet – etwa zur Gesichtserkennung, zur biometrischen Identifikation oder zur Verhaltensanalyse –, werden sie regelmäßig zu biometrischen Daten im Sinne von Art. 3 Nr. 13 JI-Richtlinie bzw. des AI Act. Sie ermöglichen dann nicht nur Identifikation, sondern auch Profilbildung und Kategorisierung, was das Ein-

griffsgewicht deutlich erhöht. Erfolgen zusätzlich Abgleiche mit polizeilichen Daten, zum Beispiel mit erkennungsdienstlichen Unterlagen, können über diese biometrischen Abgleiche Identifizierungen durchgeführt werden.

Konsequenzen für polizeiliche Systeme

Polizeiliche Systeme zur Videoüberwachung, Gesichtserkennung oder automatisierten Auswertung von Bild- und Videodaten arbeiten daher regelmäßig mit personenbezogenen und häufig mit besonderen Kategorien personenbezogener Daten. Dies gilt unabhängig davon, ob das Ausgangsmaterial aus eigenen Aufnahmen (z. B. Bodycams, stationäre Kameras), Asservaten (Mobiltelefone, Rechner, sonstige digitale Speichermedien) oder aus offen zugänglichen Quellen (Social Media, Live-streams) stammt.

Die automatisierte Verarbeitung dieser Daten ist nur auf der Grundlage bereichsspezifischer, normenklarer Ermächtigungsgrundlagen zulässig, die Datenarten, Verwendungszwecke, Speicherfristen, Zugriffsbeschränkungen, Löschpflichten und Kontrollmechanismen eindeutig regeln. KI-gestützte Funktionen (z. B. automatische Mustererkennung, Tracking, Risikobewertung) sind wegen ihrer zusätzlichen Eingriffstiefe nur zulässig, wenn die gesetzliche Grundlage sie ausdrücklich umfasst und die besonderen Risiken adressiert.

KI-gestützte Priorisierung und Vorauswertung ohne spezielle Ermächtigung

Unterschied zwischen technischer Unterstützung und eigenständigem Eingriff

Es ist verfassungsrechtlich anerkannt, dass technische Systeme als Hilfsmittel polizeilicher Sachbearbeitung eingesetzt werden dürfen, etwa zur Recherche, zur Strukturierung von Akten oder zur Visualisierung komplexer Lagen. Solange sie lediglich vorhandene Informationen in anderer Form darstellen, ohne neue grundrechtsrelevante Erkenntnisse zu generieren, liegt regelmäßig kein zusätzlicher Eingriff vor (*ATD II,* 10.11.2020).

KI-gestützte Systeme zur Priorisierung und Vorauswertung gehen aber häufig darüber hinaus. Sie generieren beispielsweise Konfidenzlevel bzw. -intervalle, Risikowerte, Ranglisten, Alerts oder Verdachtsprofile, die bestimmte Asservate, Personen oder Sachverhalte hervorheben, als besonders relevant markieren oder operative Maßnahmen vorschlagen. Zu den Risikowerten gehört zum Beispiel auch die Frage, mit welchem Konfidenzlevel geprüfte Inhalte inkriminiert sind, zum Beispiel, weil sie pädokriminelle Inhalte, verbotene Symboliken oder Waffen bzw. Betäubungsmittel abbilden können. Damit werden neue, handlungsleitende Informationen erzeugt, die nicht nur Darstellung sind, sondern Verdachtsmomente und Einschätzungen präjudizierend festlegen – etwa auch bei der Priorisierung digitaler Asservate für die Auswertung (DATAtab Team, 2025).

Steuerungswirkung und faktische Automatisierung

Auch wenn die Entscheidung formal bei menschlichen Sachbearbeitenden verbleibt, können starke algorithmische Empfehlungen de facto eine automatisierte Entscheidungsfindung bewirken. Zeitdruck, organisatorische Routinen, fehlende Transparenz der Modelle

und ein hohes Vertrauen in vermeintlich „objektive“ Technik führen dazu, dass KI-Empfehlungen selten hinterfragt werden oder faktisch nicht überprüfbar sind. So kann auch eine Negativprüfung, also die Prüfung, dass z. B. ein digitales Asservat keine inkriminierten Inhalte enthält und damit praktisch nicht weiter untersucht wird, eine automatisierte Entscheidung darstellen, wenn diese aufgrund der Empfehlung eines KI-Systems in die Sachbearbeitung übernommen wird. Gerade probabilistische Systeme, die lediglich Wahrscheinlichkeiten ausgeben, ohne ihre Kriterien offenzulegen, lassen sich im Einzelfall kaum kontrollieren. Eine kritische Prüfung der von der KI zugrunde gelegten Annahmen, Trainingsdaten und Gewichtungen ist in der Praxis schwer möglich. Die Verantwortung wird formal beim Menschen belassen, faktisch aber in erheblichem Umfang auf das System verlagert.

Diese automatisierten Bearbeitungs- und Prüfungsschritte sind in Anbetracht der Datenmengen sinnvoll und erforderlich. Gleichwohl müssen die Risiken und faktischen Auswirkungen sowohl rechtlich als auch praktisch umfassend berücksichtigt werden.

Erforderlichkeit einer eigenen Ermächtigungsgrundlage

Vor diesem Hintergrund ist die Annahme unzutreffend, KI-gestützte Priorisierung und Vorauswertung sei ohne eigene Ermächtigungsgrundlage zulässig, solange keine unmittelbar belastenden Entscheidungen automatisiert getroffen werden. Soweit die Systeme neue Verdachtsmomente, Risikoprofile oder Personenkategorien erzeugen, die weitere (Gefahren-) Ermittlungsschritte nach sich ziehen, liegt ein eigenständiger Eingriff in das Recht auf informationelle Selbstbestimmung vor. Auch bei einer Negativabgrenzung, zum Beispiel durch Aussortieren digitaler Asservate als nicht relevant, liegt faktisch eine automatisierte Entscheidung vor, auch wenn diese normativ durch Menschen bestätigt werden muss. Praktisch dürfte eine Einzelfallprüfung hier nicht möglich sein.

Bei starker Steuerungswirkung können auch menschenwürdebezogene Aspekte berührt sein.

Verfassungsrechtlich geboten ist daher eine ausdrückliche, hinreichend bestimmte gesetzliche Grundlage, die insbesondere regelt, zu welchen Zwecken KI-basierte Analyse- und Priorisierungssysteme eingesetzt werden dürfen, welche Datenkategorien herangezogen werden dürfen und welche ausgeschlossen sind, welche Eingriffsschwellen (Gefahrengrad, Verdachtsniveau) gelten, welche methodischen Grenzen (z. B. Verbot selbstlernender Systeme in bestimmten Einsatzbereichen) zu beachten sind, welche Transparenz- und Dokumentationspflichten gelten und wie retrograd kontrolliert wird sowie welche Rechte Betroffene (Auskunft, Korrektur, Widerspruch) haben. Ohne eine solche spezifische Ermächtigung ist der Einsatz von KI-Systemen zur Priorisierung und Vorauswertung im polizeilichen Gefahrenabwehr- und Strafverfolgungsbereich verfassungsrechtlich hochproblematisch.

Training und „Untraining“ von KI-Systemen

Das Training von KI-Systemen ist eigenständig Bias-gefährdet. Sowohl die Auswahl der Trainingsdaten als auch die Ergebnisbewertung bedürfen besonderer Aufmerksamkeit. Da der polizeiliche Fokus regelmäßig auf gefahrengeneigten oder strafrechtlich relevanten Daten liegt, kann hier eine Verzerrung bereits bei der Auswahl bzw. Verfügbarkeit von Trainingsdaten eintreten. Werden Echtdaten zum Training von KI-Systemen eingesetzt, gehen die Einschät-

zungen darüber, ob es sich bei dem dann vorliegenden Großen Sprachmodell oder Large Language Modell um ein personenbezogenes Datum handelt oder nicht, auseinander. Während der Hamburgische Beauftragte für Datenschutz keine Persönlichkeitsrelevanz sieht (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, S. 8), argumentiert der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, dass KI-Modelle Trainingsdaten memorisieren und durch offensive Fragetechniken diese ausgeben können und diese damit deanonymisieren. Dieser Einschätzung folgt auch die Universität Tübingen und geht davon aus, dass Trainingsdaten in KI-Modellen, wenn auch nicht als „klassische" Datensätze, gespeichert werden (Nolte et al., 2025, S. 1). Dem „Anspruch auf Vergessen" kann dabei auf zwei unterschiedliche Weisen begegnet werden. Zum einen durch „unlearning" (Keber et al., 2024, S. 9). Dabei werden die zum Training genutzten Datensätze aus dem Modell entfernt. Da aber generative Modelle den Umgang mit diesen Daten lernen, kann es bei Ausgaben immer noch zu verblüffenden Ähnlichkeiten kommen, weshalb hier die Unterdrückung dieser Datensätze bei der Verarbeitung von Anfragen (Prompts) als Mittel zum Einsatz kommt (datenschutzticker.de, 2025). Bei beiden Mitteln ist die technologische Umsetzung allerdings derzeit noch nicht so weit gediehen, dass von einer rechtskonformen Umsetzung der Löschung von Trainingsdaten aus KI-Modellen ausgegangen werden kann.

Verknüpfung offen zugänglicher Daten (OSINF/OSINT) mit polizeilichen Datenbeständen

Abgrenzung: bloße Internetaufklärung vs. automatisierte Erhebung

Das BVerfG differenziert zwischen bloßer „Internetaufklärung", Datenerhebung und strukturierten, automatisierten Datenverarbeitungsmaßnahmen. Ein reines, manuelles „Surfen" von Polizeibeamtinnen und -beamten auf öffentlich zugänglichen Webseiten, ohne konkretisierten Ermittlungszweck und ohne technischen Erfassungsakt, wird als schlichte Kenntnisnahme eingestuft und begründet für sich genommen noch keinen Eingriff in das Recht auf informationelle Selbstbestimmung (*Onlinedurchsuchung,* 2008, RN. 308 ff. m. w. N.).

Sobald jedoch Daten gezielt – manuell oder automatisiert – erhoben, gespeichert, strukturiert oder für spätere Auswertungen vorgehalten werden, liegt – unabhängig vom öffentlich zugänglichen Ursprung – eine Verarbeitung personenbezogener Daten vor. Schon eine dreistufige Verarbeitung (Erhebung, Speicherung, Abruf) überschreitet die Schwelle der bloßen Kenntnisnahme deutlich, unabhängig davon, ob sie manuell oder automatisiert erfolgt. Eine Automatisierung einzelner Verarbeitungsschritte oder der Einsatz von KI-Komponenten intensiviert die jeweiligen Handlungen eigenständig.

OSINT/OSINF und automatisierter Abgleich

Offen zugängliche Informationen aus Social-Media-Plattformen, Foren, Blogs oder Nachrichtenportalen (OSINF/OSINT) können inhaltlich hochsensibel sein: Sie betreffen nicht nur allgemeine Meinungen, sondern auch politische Überzeugungen, Teilnahme an Versammlungen, soziale Beziehungen, Lebensstil, Beruf und vieles mehr. Werden solche Daten gesammelt, separat oder aggregiert in Polizeidatenbanken übernommen und mit vorhande-

nen Beständen – etwa Meldedaten, Strafakten, Bewegungsdaten – abgeglichen, erhöht sich das Eingriffsgewicht erheblich. Erfolgen diese Schritte automatisiert, erhöht sich das Eingriffsgewicht jeweils separat.

Die automatisierte Verknüpfung offen zugänglicher Daten miteinander oder mit polizeilichen Datenbeständen ermöglicht die Erstellung umfassender Persönlichkeits- und Bewegungsprofile, die weit über das hinausgehen, was Betroffene beim Posten einzelner Inhalte erwarten können. Sie verschiebt die Grenze zwischen öffentlicher Selbstdarstellung und staatlich orchestrierter Wissensproduktion (*Automatisierte Datenanalyse,* 16.02.2023).

Verfassungsrechtlich folgt daraus: Der Umstand, dass Daten öffentlich zugänglich sind, hebt den Grundrechtsschutz nicht auf. Auch öffentlich gemachte Informationen können durch staatliche Erhebung, Speicherung, Aggregation und Profilbildung grundrechtsrelevant werden. Automatisierte OSINT-Verarbeitung und Abgleich mit polizeilichen Beständen stellen regelmäßig einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar und bedürfen einer speziellen gesetzlichen Grundlage. Eingriffsschwellen, Zweckbindung, Speicherfristen, Zugriffsbeschränkungen und Kontrollmechanismen müssen besonders strikt ausgestaltet werden, da Streubreite, Heimlichkeit und Profilbildungspotenzial hoch sind.

Keine Datenerhebung und -speicherung auf Vorrat

Das BVerfG hat wiederholt klargestellt, dass die Sammlung personenbezogener Daten „auf Vorrat“ zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungswidrig ist. Offene Datenpools, deren spätere Nutzung erst nachträglich festgelegt oder weitgehend der Exekutive überlassen wird, bergen ein erhebliches Missbrauchspotenzial und sind mit dem Bestimmtheitsgebot unvereinbar.

Für automatisierte und KI-gestützte Verfahren bedeutet dies, dass Datenbestände nicht allein geschaffen werden dürfen, um künftige, noch unbestimmte Analyseoptionen zu eröffnen. Je unbestimmter die Speicher- und Nutzungszwecke, desto höher das Eingriffsgewicht und desto restriktiver die verfassungsrechtliche Bewertung (*Telekommunikationsüberwachung I,* 14.07.1999, RN 167 m. w. N.).

Kein „Freifahrtschein“ durch öffentliche Quellen

Auch das Selbstoffenbaren von Daten im Internet führt nicht zu einem Wegfall grundrechtlichen Schutzes. Das Recht auf informationelle Selbstbestimmung schützt nicht nur die Geheimhaltung, sondern auch vor staatlicher Aggregation, Profilbildung und Anschlussnutzung öffentlich zugänglicher Informationen. Entscheidend ist die neue Informationslage, die der Staat durch seine Datenverarbeitung schafft.

Daraus folgt insbesondere: Automatisierte Erhebung und Auswertung öffentlich zugänglicher Daten – etwa durch Crawler, Scraper oder KI-gestützte Analysewerkzeuge – begründen einen Eingriff. Der Abgleich mit anderen Datenbeständen (Melderegister, polizeiliche Ver-

bunddateien, Telekommunikationsdaten) verstärkt das Eingriffsgewicht weiter. Es bedarf bereichsspezifischer Ermächtigungsgrundlagen mit hohen Eingriffsschwellen, insbesondere wenn die Daten zur operativen Aufgabenwahrnehmung genutzt werden sollen.

Spezielle verfassungsrechtliche Leitplanken für automatisierte und KI-gestützte polizeiliche Datenverarbeitung

Sowohl automatisierte Datenauswertung und -analyse als auch der Einsatz von KI-Systemen oder von Systemen mit KI-Komponenten stellen besonders eingriffsintensive Techniken und Methoden dar. Dabei ist es unerheblich, ob es sich um deterministische oder probabilistische Systeme handelt. Der Einsatz dieser Systeme ist eigenständig zu betrachten.

Automatisierte Datenanalyse – gleich ob traditionell regelbasiert oder KI-gestützt – ist nicht bloße Fortsetzung menschlicher Auswertung mit effizienzsteigernden Werkzeugen, sondern entfaltet eine eigenständige Eingriffsqualität, da sie neue, verdichtete Informationen erzeugt. Dies gilt etwa für Clusteranalysen und Netzwerkgraphen, die Beziehungen zwischen Personen sichtbar machen, für Bewegungs- und Kommunikationsprofile, statistische Risikomodelle und scoringbasierte Gefährlichkeitsprognosen oder Mustererkennung in Bild- und Videodaten, die Verhalten oder Emotionen interpretieren.

Der Gesetzgeber muss Art und Umfang der zulässigen Analysen, die zugrunde liegenden Datenbestände und die Reichweite profilbildender Verfahren gesetzlich konkret begrenzen. Besonders leistungsfähige oder intransparente Systeme – etwa selbstlernende KI – erfordern zusätzliche Sicherungen bis hin zu ausdrücklichen Verboten in bestimmten Einsatzbereichen.

Aus der dargestellten Rechtsprechung ergeben sich besondere Anforderungen für KI-spezifische Ermächtigungsgrundlagen im Polizeirecht. Mindestanforderungen, die sich aus den Urteilen des BVerfG ableiten, sind:

KI-Einsatz darf nicht in allgemeinen Generalklauseln versteckt werden, sondern muss in speziellen Normen mit klar umrissenen Anwendungsfeldern geregelt sein (bereichsspezifische Normierung).

Die Norm muss konkret festlegen, für welche Zwecke die KI eingesetzt werden darf (z. B. Gefahrenabwehr in klar definierten Konstellationen, nicht: „Optimierung polizeilicher Arbeit“).

Es ist festzulegen, welche Daten genutzt werden dürfen (z. B. bestimmte polizeiliche Bestände, bei Automatisierung explizit bezeichnete OSINT-Quellen) und welche ausgeschlossen sind (z. B. besonders schutzwürdige Daten ohne qualifizierten Anlass).

Die Eingriffsschwellen (konkretisierte Gefahr, dringende Gefahr, Anfangsverdacht) müssen an Eingriffstiefe und Sensibilität der Daten angepasst werden.

Methodische Grenzen sind vorzusehen, etwa Verbote selbstlernender Systeme in besonders sensiblen Bereichen oder der Ausschluss bestimmter Profiling- oder Kategorisierungsverfahren (z. B. biometrische Kategorisierung nach Herkunft oder Religion).

Transparenz, Dokumentation und Kontrolle sind durch Protokollierung, interne und externe Aufsicht (Datenschutzbeauftragte, unabhängige Gremien), Benachrichtigungs- und Auskunftsrechte für Betroffene sowie regelmäßige Evaluierung von Fehler- und Bias-Risiken sicherzustellen.

Schließlich ist der Schutz des Kernbereichs privater Lebensgestaltung zu gewährleisten: Bestimmte Datenkategorien und Verarbeitungsweisen, die diesen Kernbereich betreffen würden, sind auch bei schwersten Gefahren auszuschließen.

Schlussbemerkung

Die polizeiliche Datenverarbeitung steht im Spannungsfeld zwischen wirksamer Gefahrenabwehr und Strafverfolgung einerseits und dem Schutz der Freiheitsrechte andererseits. Automatisierte und KI-gestützte Systeme verschärfen dieses Spannungsfeld, weil sie sowohl erhebliche Chancen als auch qualitativ neue Risiken mit sich bringen. Europa- und verfassungsrechtlich zulässig ist ihr Einsatz nur, wenn Ermächtigungsgrundlagen die Eingriffsschwellen und die Eingriffstiefe differenziert berücksichtigen, Bilder und Videos als personenbezogene bzw. biometrische Daten angemessen schützen, KI-basierte Priorisierungen auf eine klare gesetzliche Grundlage stellen und die automatisierte Verknüpfung offen zugänglicher Daten mit polizeilichen Beständen strengen Schranken unterwerfen.

Referenzen

Ackerschott, F. S. (2026). Cyberrecherche 2.0: Der Leitfaden für KI-Gestützte Open Source Intelligence, Ermittlung & Recherche. Springer Fachmedien Wiesbaden.

DATAtab Team (Hrsg.). (2025). Konfidenzintervall. https://datatab.de/tutorial/konfidenzintervall

datenschutzticker.de (Hrsg.). (2025). Machine Unlearning: Die Lösung für das Recht auf Vergessenwerden? https://www.datenschutzticker.de/2025/11/memorisierung-personenbezogener-daten-in-ki-llm/

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. (2024). Diskussionspapier: Large Language Models und personenbezogene Daten. https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf

Keber, T., Wacke, J., Herzog, Y., Kicherer, W., Meding, K., Nägele, P., Maslewski, D., Rembold, J., Skobel, E., & Steinbrück, A. (2024). Unsere Freiheiten: Daten nützen – Daten schützen: Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz.

Kunze, D. (2026). KI-Einsatz bei der Polizei. In K. Chibanguza, C. Kuß & H. Steege (Hrsg.), NomosHandbuch. Künstliche Intelligenz: Recht und Praxis automatisierter und autonomer Systeme | Generative KI. Rechtshandbuch (2. Auflage, S. 1439–1469). Nomos.

Nolte, H., Finck, M., & Meding, K. (2025). Machine Learners Should Acknowledge the Legal Implications of Large Language Models as Personal Data. Universität Tübingen, Tübingen. https://arxiv.org/pdf/2503.01630

Rechtsprechung

ATD II, 1 BvR 3214/15, BVerfGE 156, 11 (Bundesverfassungsgericht 10. November 2020). https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2020/11/rs20201110_1bvr321415.pdf;jsessionid=3C3C1CB11DE9CB9438E17C9A45AC004B.internet951?__blob=publicationFile&v=2

Automatisierte Datenanalyse, 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363 (Bundesverfassungsgericht 16. Februar 2023). https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2023/02/rs20230216_1bvr154719.pdf?__blob=publicationFile&v=1

Automatisierte Entscheidungsfindung – Begründung, C-203/22 (Europäischer Gerichtshof 12. September 2024).

Automatisierte Kennzeichenerfassung, 1 BvR 2074/05, BVerfGE 120, 378 (Bundesverfassungsgericht 11. März 2008).

Bestandsdatenauskunft II, 1 BvR 1873/13, 1 BvR 2618/13, BVerfGE 155, 119 (Bundesverfassungsgericht 27. Mai 2020).

BKAG, HyDane, 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220 (Bundesverfassungsgericht 20. April 2016).

Journalistische Verbindungsdaten, 1 BvR 330/96, 348/99, BVerfGE 107, 299 (Bundesverfassungsgericht 12. März 2003).

Mediziner-BAföG, 1 BvR 2035/07, BVerfGE 129, 49 (Bundesverfassungsgericht 21. Juni 2011).

Onlinedurchsuchung, 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 (Bundesverfassungsgericht 27. Februar 2008).

Rasterfahndung II, 1 BvR 518/02, BVerfGE 115, 320 (Bundesverfassungsgericht 4. April 2006).

Solange I, 2 BvL 52/71, BVerfGE 37, 271 (Bundesverfassungsgericht 29. Mai 1974).

Solange II, 2 BvR 197/83, BVerfGE 73/339 (Bundesverfassungsgericht 22. Oktober 1986).

Telekommunikationsüberwachung I, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313 (Bundesverfassungsgericht 14. Juli 1999).

Van Gend en Loos v Administratie der Belastingen, C-26/62, 1 Slg. 163 (EuGH 5. Februar 1963). https://curia.europa.eu/juris/showPdf.jsf?text=&docid=87120&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=772103

Volkszählungsurteil, 1 BvR 209/83, 1 BvR 269/83. 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (Bundesverfassungsgericht 15. Dezember 1983).

Zuordnung dynamischer IP-Adressen, 1 BvR 1299/05, BVerfGE 130, 151 (Bundesverfassungsgericht 24. Januar 2012).

Die Entwicklung der polizeilichen Presse- und Öffentlichkeitsarbeit – Von Brief und Fax bis zum crossmedialen Kommunikationsmanagement und zur Professionalisierung der Mitarbeitenden

Stefan Jarolimek

Die polizeiliche Presse- und Öffentlichkeitsarbeit ist heutzutage vielfältig. Neben der klassischen Pressearbeit steht der Organisationskommunikation heute ein Bündel an multimedialen Instrumenten zur Verfügung: Intranet, Social-Media-Kanäle, Gaming-Plattformen, professional networks, Podcasts. Damit verbunden ist eine rasante medientechnologische Entwicklung, die immer wieder neue Geräte, Räumlichkeiten und Kompetenzen erfordert – nicht zuletzt, um die Vielzahl der Möglichkeiten beispielsweise in einem Newsroom zu bündeln, der wiederum mit einem digitalen Netzwerk hinterlegt ist.

Der vorliegende Beitrag zeichnet die Entwicklung der polizeilichen Presse- und Öffentlichkeitsarbeit nach. Er setzt vor dem 21. Jahrhundert an, um auch die Anfänge zu beleuchten und die rasante Entwicklung in den vergangenen zwei Dezennien zu verdeutlichen. Der Abriss beginnt mit der Entstehung der ersten Pressestellen von Unternehmen zu Beginn des 20. Jahrhunderts und beschreibt Vorläufer der Pressemitteilungen als erste Medientechnik.

Die Pressearbeit der entmilitarisierten Polizei nach dem Zweiten Weltkrieg beginnt in den 1950er Jahren, was anhand des Polizeipräsidiums Mainz nachgezeichnet wird. Telefon und später das Faxgerät sind über Jahrzehnte die technischen Hilfsmittel der Pressestellen. Die akzelerierte Entwicklung setzt Ende der 1990er Jahre ein und nimmt in den 2010er Jahren Fahrt auf: Internet und Social Media, Smartphones und Laptops prägen heute nicht nur die Gesellschaft, sondern auch die Arbeit der Polizei. In den vergangenen 20 Jahren wird eine zunehmende Professionalisierung und strategische Ausrichtung sicht- und messbar.

Schließlich soll am Ende des Artikels auf aktuelle Entwicklungen eingegangen werden. Mit Twitch bedient eine erste deutsche Polizei eine Gaming-Plattform, die ganz andere Technik benötigt. Und wenig überraschend zieht die Künstliche Intelligenz in die Presse- und Öffentlichkeitsarbeit ein, deren Verwendung an einigen Beispielen verdeutlicht werden soll.

Entstehung und Entwicklung von Pressestellen und Public Relations

Die ersten Pressestellen entstehen Ende des 19. Jahrhunderts auch infolge der Industrialisierung und der Professionalisierung des Journalismus. Zuvor sind es Großunternehmer wie Krupp, der sich teils über die Berichterstattung ärgert und in der Folge Anzeigen in Zeitungen schaltet, um seine eigene Darstellung zu publizieren. Später bezahlt er verdeckt Journalisten und Publizisten für eine positive Darstellung in der Berichterstattung (u. a. Oeckl, 1987, Kunczik, 2009). Vorbereitet von den Unternehmensgründern Alfred Krupp und Werner von Siemens entstehen in den Betrieben 1893 und 1902 sogenannte Nachrichtenbüros (vgl. Kunczik, 2009).

Technisch sind diese rudimentär ausgestattet. Im Journalismus stellen neben telegrafischen Agenturen vor allem Korrespondenzen wichtige Informationsquellen dar. Spezialisierte Verlage, aber auch Einzelpersonen liefern Neuigkeiten zu unterschiedlichen Themen: von politischen Nachrichten bis hin zu Unternehmensinformationen. Korrespondenzen werden meist als fertige Artikel postalisch versandt und häufig von den Redakteuren zerschnitten und neu mit Ergänzungen und Änderungen zusammengesetzt. Daher sind Korrespondenzen in der Wilhelminischen Ära als historische Quelle schwer zu fassen. Erst später werden sie durch Verzeichnisse der Redaktionen und Anbieter nachvollziehbar.

„Die Zahl dieser Verzeichnisse erhöhte sich in den 1920er Jahren. Diese Entwicklung verweist einerseits auf die gestiegene funktionale Bedeutung der Korrespondenz als Materiallieferant für die Presse, als Mittel der Öffentlichkeitsarbeit wie auch als journalistisches Arbeitsfeld und andererseits auf die fortschreitende Standardisierung der Erhebungen durch fachliche Experten“ (Kutsch et al., 2011, S. 163).

Der Begriff und die Methoden der Public Relations als strategische Kommunikation bleiben in Deutschland lange unbekannt. In den 1920er Jahren arbeitet die IG Farben mit dem amerikanischen PR-Berater Ivy Lee zusammen, der als einer der Väter der modernen Public Relations gilt. Lee unterstützt in dieser Zeit auch aktiv die NSDAP bis 1934. Nach seiner Rückkehr in die USA muss er sich dafür vor dem US-Kongress verantworten.

Mit der Machtergreifung der NSDAP folgt die staatliche Propaganda. In Deutschland übersetzt man Public Relations aufgrund der politisch ungewollten englischen Sprache ins Deutsche: Öffentlichkeitsarbeit. Carl Hundhausen (1951) legt in dieser Zeit einen wichtigen Grundstein mit seinem Buch „Werbung um öffentliches Vertrauen. Public Relations“, das das Berufsfeld theoretisch einordnet.

Nach dem Zweiten Weltkrieg folgen Neubeginn und Aufschwung. Vor allem PR-Praktiker wie Albert Oeckl tragen mit ihren Schriften zur theoretischen Grundlage bei. Oeckl beschreibt Mitte der 1960er Jahre, dass die Aufgabe der PR/Öffentlichkeitsarbeit darin bestehe, „die Informationslage der Gesellschaft zu verbessern. Sie solle dem einzelnen Orientierungshilfen in der ‚hoch differenzierten Gesellschaft‘ geben und den für das Funktionieren von Demokratie nötigen politischen und sozialen Konsens herstellen“ (Kunczik, 2009, S. 235).

Die folgenden Phasen der Professionalisierung und auch PR-Wissenschaft sollen hier verkürzt und danach am Beispiel der Polizei dargestellt werden. Bentele (1997, 2013) systematisiert die Entwicklung der Public Relations in Deutschland in folgende Perioden:

- Vorgeschichte: Staatliche Pressepolitik, funktionale PR, Entwicklung eines Instrumentariums
- Mitte 19. Jh.–1918 - 1. Periode: Entstehung des Berufs, Entwicklung erster Presseabteilungen in Politik, Wirtschaft und Kriegsarbeit
- 1918–1945 – 2. Periode: Konsolidierung und Wachstum: Ausbreitung von Presseabteilungen in diversen gesellschaftlichen Bereichen: Wirtschaft, Politik, Verwaltung
- 1933–1945 – 3. Periode: NS-Pressearbeit: Parteiideologisch dominierte Pressearbeit im Rahmen politischer Propaganda

- 1945−1958 – 4. Periode: Neubeginn und Aufschwung: Orientierung an amerikanischen Vorbildern; Entwicklung eines beruflichen Selbstverständnisses
- 1958−1985 – 5. Periode: Konsolidierung des Berufsfelds: Entwicklung eines beruflichen Selbstbewusstseins; Gründung des Berufsverbands Deutsche Public Relations Gesellschaft (DPRG)
- 1985−1995 – 6. Periode: Boom des Berufsfeldes, Professionalisierung: Starke Entwicklung des PR-Agentursektors; Akademisierung und Professionalisierung des Berufsfelds
- Ab 1995 – 7. Periode: Einfluss des Internets, Globalisierung, Social Media: Auswirkungen des Internets auf die Kommunikation von Organisationen, Internationalisierung der Kommunikation

Innerhalb der deutschen Polizeien startet die Presse- und Öffentlichkeitsarbeit in der Fläche mit der Entmilitarisierung nach dem Zweiten Weltkrieg, wie im folgenden Kapitel am Beispiel der Polizei Mainz gezeigt wird.

Entwicklung von Pressestellen der Polizei am Beispiel Mainz

Im Vergleich zu den bereits genannten Großunternehmen beginnt eine Ausbreitung der Presseabteilungen in der Polizei erst nach dem Zweiten Weltkrieg. Bislang liegen kaum Arbeiten vor, die im Speziellen die Entwicklung der Pressestellen oder der Kommunikation der Polizei nachzeichnen (eine Ausnahme bildet u. a. zu Social Media Graßl, 2023).

Kunz (2018) beschreibt diese Entwicklung für das Polizeipräsidium Mainz auf Basis von polizeiinternen Quellen und Zeitzeugeninterviews. Er unterteilt sie in grobe Phasen von einem oder zwei Jahrzehnten und orientiert sich in der Beschreibung an den beschriebenen Perioden von Bentele.

Die 1950er Jahre – Neuorientierung und erste Schritte

Das älteste recherchierte Dokument zur Presse- und Öffentlichkeitsarbeit datiert auf das Jahr 1950, das Rahmenbedingungen kriminalpolizeilicher Presse- und Rundfunkveröffentlichungen umfasst. Jede Veröffentlichung ist weiterhin in Absprache mit dem Innenministerium zu tätigen. Auskunftsberechtigt sind zudem ausschließlich Führungskräfte. Nach weiteren Erlassen, die auch eine proaktive Kommunikation erlauben, und ähnlichen Entwicklungen in weiteren rheinland-pfälzischen Präsidien wird 1958 der erste Pressesprecher eingestellt. Das Aufgabenspektrum ist zunächst unklar, weshalb die Stelle mit Verkehrsangelegenheiten zusammengelegt wird (Kunz, 2018, S. 18).

Technisch steht das Telefon im Vordergrund. Mit ihm stellt der Pressesprecher Kontakt zu den lokalen und regionalen Journalisten her. Später geht er dazu über, täglich Journalisten zu Gesprächen persönlich einzuladen, um die Kontakte zu intensivieren.

Die 1960er Jahre – Entwicklung des Berufsfelds in der Polizei

Die Entstehung von vollwertigen Pressestellen kommt vor allem durch die hohe Belastung des Behördenleiters auf. Der Polizeipräsident Ellscheid richtet 1965 die erste Pressestelle in Mainz ein (vgl. Kunz, 2018, S. 20). Der Pressesprecher ist nun fester Bestandteil der neuen Abteilung, die Verkehrsangelegenheiten gehören nicht mehr zur Funktion. Die Bedeutung der Presse und des Rundfunks wächst. Als einziger „Nicht-Exekutiver" nimmt der Pressesprecher an den morgendlichen Besprechungen beim Polizeipräsidenten teil. Weiterbildungen erhalten die Mitarbeiter in der Pressestelle nicht.

Die 1970er und 1980er Jahre – Verstetigung und Wachstum

In den 1970er Jahren werden die Presseabteilungen verstetigt und finden sich nun auch in den Organisationsübersichten. Die Pressestellen erhalten die Kennzeichnung Z/3 (vgl. das Beispiel aus Koblenz in Abb. 1).

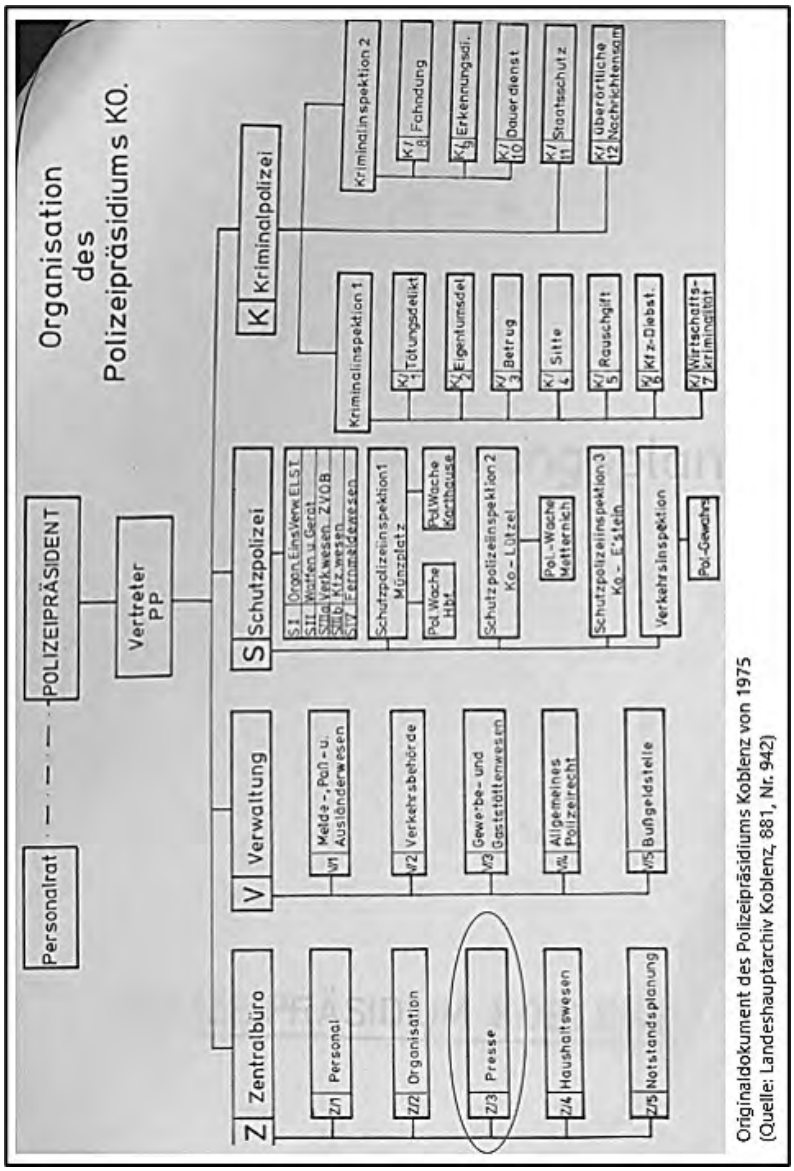


Abb. 1: Organisationsplan des Polizeipräsidiums Koblenz 1975 (aus Kunz, 2018, S. 21)

„In Mainz definiert die Staatskanzlei erstmals das Handlungsfeld Presse- und Öffentlichkeitsarbeit in der Verwaltung. Instrumente der Pressearbeit sowie Formen und Techniken der Öffentlichkeitsarbeit werden jetzt beschrieben. ‚Pressearbeit ist eine Führungsaufgabe; der Pressereferent ist an ihr beteiligt, er kann sie aber nicht allein wahrnehmen'" (Kunz, 2018, S. 21). Einzelne Tarifangestellte – meist von der Presse kommend – ergänzen erstmals die Pressestelle. Mit der Konsolidierung und dem anfänglichen Boom des Berufsfeldes werden in Stellenanzeigen „Journalisten" für Pressestellen gesucht, die in der PR-Geschichte meist als die „anderen" Journalisten oder als PR-Journalisten bezeichnet werden (Szyska, 1990).

Die Zeitzeugen aus Rheinland-Pfalz beschreiben als Grundlage zur Informationsbeschaffung vor allem die persönlichen Kontakte im Präsidium, die sie bei morgendlichen Rundgängen durch das Haus erledigen. Eine interne Kommunikation ist noch kaum zu erkennen.

Technisch stellt die Verbreitung des Faxgeräts Mitte der 1980er Jahre auch für die Pressestelle eine wesentliche Veränderung dar. Das Versenden und Empfangen von Informationen ist nun viel schneller und an einen größeren Adressatenkreis möglich. In einigen Pressestellen hält sich das Fax bis in die 2000er Jahre.

Die 1990er und 2000er Jahre – Das Internet verändert alles

Im Zuge verschiedener Reformen in der Polizei Rheinland-Pfalz, insbesondere in den Jahren 1993 und 1997, legen auch die Bereiche der Presse- und Öffentlichkeitsarbeit Vorschläge für Veränderungen vor. „Die Arbeitsgruppe Presse- und Öffentlichkeitsarbeit der Polizei in Rheinland-Pfalz legt im Herbst 1993 einen Vorschlag zur künftigen organisatorischen, personellen und strategischen Ausrichtung der Presse- und Öffentlichkeitsarbeit bei der rheinland-pfälzischen Polizei vor. Demnach sind auch bei der künftigen Organisationsform der Polizeipräsidien die Behördenleiter für die Aufgaben der Presse- und Öffentlichkeitsarbeit unmittelbar zuständig. Ihnen wird zur Wahrnehmung dieser Führungsaufgabe unmittelbar eine Pressestelle zugeordnet" (Kunz, 2018, S. 22).

Technisch ermöglicht das Internet erstmals, Informationen als Organisation ohne den Umweg über den Journalismus und neben gedruckten Broschüren unmittelbar einem breiten Publikum zu präsentieren. Mitarbeitendeninformationen werden nun per E-Mail verschickt oder online im Intranet publiziert, aber nicht mehr postalisch zugestellt.

Kommunikation in der Polizei Rheinland-Pfalz heute (Stand 2018)

Die 2018 von Kunz verfasste Arbeit beschreibt die Presse- und Öffentlichkeitsarbeit am Ende noch einmal zum Zeitpunkt der Bearbeitung. Als eine der ersten Polizeien in Deutschland richtet Rheinland-Pfalz eine Koordinierungsstelle Kommunikation ein, die insbesondere strategische Fragen rund um das Internet (inklusive Social Media) und Intranet bearbeitet (vgl. Abbildung 2). Geleitet wird diese Stelle von einem Polizeibeamten bzw. einer Polizeibeamtin im vierten Einstiegsamt (ehemals höherer Dienst); zudem wurde eine Tarifangestellte/ein Tarifangestellter als Redakteur*in eingestellt.

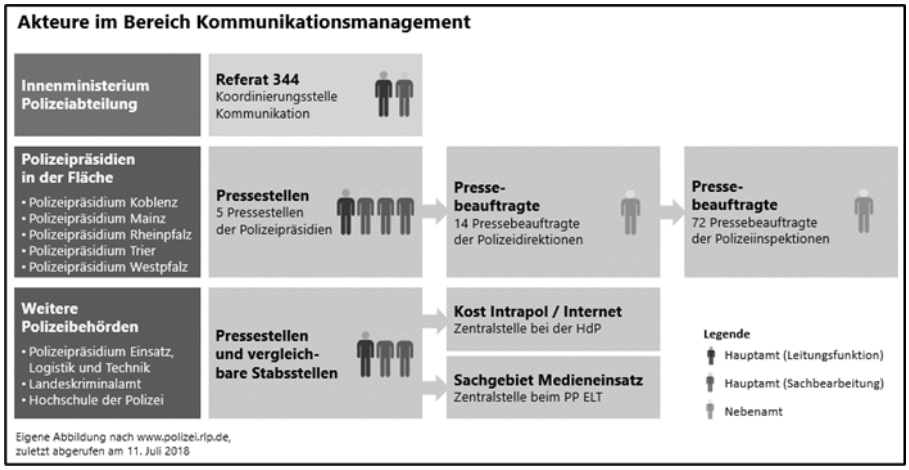


Abb. 2: Akteure im Kommunikationsmanagement in Rheinland-Pfalz 2018 (nach Kunz, 2018, S. 13)

„Die zentrale Aufgabe der neuen Koordinierungsstelle ist die Entwicklung und Umsetzung einer landesweiten Kommunikationsstrategie zu den Themenfeldern externe und interne Kommunikation. Zudem sollen alle Akteure und Bedarfsträger identifiziert und vernetzt sowie deren Zusammenarbeit koordiniert werden. Letztendlich soll die strategische Steuerung der Organisationskommunikation durch die Koordinierungsstelle Kommunikation der Polizei geleistet werden. Die Projektziele betreffen gleichermaßen den Bereich der externen Öffentlichkeitsarbeit/Public Relations und den Bereich der internen Kommunikation“ (Kunz, 2018, S. 23).

Die Arbeit von Kunz endet in einer Phase, in der die Polizeien neben Internet und teils noch rudimentären Intranetauftritten zunehmend das Themenfeld Social Media entdecken, was vermutlich den größten Wandel in den Abteilungen der Presse- und Öffentlichkeitsarbeit mindestens seit den 1990er Jahren bedeutet.

Social Media und professionelles Intranet seit den 2010er Jahren: Ausweitung, Professionalisierung, Medientechnik, Strategische Kommunikation

Die Social-Media-Kommunikation der deutschen Polizeien beginnt zaghaft. Häufig sind es anfangs einzelne Polizisten oder Projektgruppen, die Social Media, zu Beginn insbesondere Facebook und Twitter, bespielen.

Social Media

2013 beschließt der Unterausschuss Führung, Einsatz und Kriminalitätsbekämpfung (UAFEK) als Untergremium der Innenministerkonferenz grundsätzliche Regeln für die Social-Media-Kommunikation der Polizeien, die von einer Bund-Länder-Projektgruppe erarbeitet wurden. Demnach soll ein Konzeptpapier vorliegen, bevor die Social-Media-Kommunikation startet.

Im November 2015 findet der erste bundesweite Social Media Best Practice Workshop der deutschen Polizeien statt. In einem noch überschaubaren Kreis stellt vor allem die Polizei Berlin ihr Vorgehen vor. Das einen Monat zuvor an der Deutschen Hochschule der Polizei gegründete Fachgebiet Kommunikationswissenschaft organisiert seit 2016 ein Barcamp

Social Media (ab 2025 Presse- und Öffentlichkeitsarbeit). Mit dem von den Polizeien veranstalteten Best Practice im Herbst und dem Barcamp im Frühjahr diskutieren alle deutschen Polizeien zweimal im Jahr die aktuellen Herausforderungen in der schnelllebigen Social-Media-Kommunikation.

Die Ausweitung in allen Polizeien bedeutet eine vor allem auch personelle Aufwertung der Kommunikationsabteilungen. In Berlin und München arbeiten mittlerweile über 30 Personen. Mit Social Media setzen viele Polizeien nun verstärkt auf externe Kräfte, die Kompetenzen aus spezialisierten Studiengängen, Agenturen oder dem (Online-)Journalismus in die Polizeien tragen. Damit steigt auch der Grad der Akademisierung. Teilweise werden neue Strukturen in den P/ÖA-Abteilungen notwendig, um die schnelle Kommunikation über Social Media auch intern abzubilden. Die (Teil-)Einführung von Corporate Newsrooms ist dafür ein Zeichen (vgl. Sadrowski & Jarolimek, 2016; Moss, 2022; Erler, 2020).

Die technischen Anforderungen steigen im Vergleich zu der Vor-Social-Media-Zeit erheblich. Die Presseteams benötigen „freie“ Smartphones, Tablets und neben den Polizeirechnern zusätzliche „freie“ Rechner mit Internetzugang.

Zur Produktion von Videos, vor allem für die hochwertigen Formate bei YouTube und Facebook, werden digitale Spiegelreflexkameras, hochwertige Mikrofone, GoPros, Drohnen und vieles mehr angeschafft.

Neben der Hardware ist auch die Software zu Beginn von Social Media häufig eine Herausforderung. Benötigt werden Lizenzen für Community Management Tools (Social Hub oder Facelift), Bildbearbeitungs- und Grafikprogramme, Videoschnitt, Tools zur Zusammenarbeit. Zum Teil kämpfen die Mitarbeitenden mit neuer Software, die auf alten Windows-Rechnern nicht mehr richtig funktioniert.

Die technologischen Anforderungen ändern sich auch mit den Kanälen. Mit dem Aufkommen von bild- und bewegtbildzentrierten Social-Media-Kanälen wie Instagram verlagern sich Veröffentlichungen stark auf diese zu Beginn noch hochwertigen Bild- und Videoformate. Mit TikTok und auch der Entwicklung der Smartphone-Kameras und integrierter Bildbearbeitungsprogramme verändern sich diese. TikTok setzt auf schnell produzierte, authentische und kurze Beiträge, die auch einfach mal mit dem Handy gefilmt und geschnitten werden, mit kleinem Ansteckmikrofon aufgenommen. Nach dem Erfolg von TikTok setzt sich dieser Trend auch bei Facebook, Instagram und YouTube (YouTube shorts) durch.

Intranet

Social Media hat auch einen Einfluss auf die interne Kommunikation. Zum einen erhöhte die schnelle 24/7-Kommunikation den Druck, auch intern schnell kommunizieren zu können; zum anderen ändern sich die Mediennutzungsgewohnheiten allgemein. Kurze, einfach verfügbare Texte, bildhaft und mit Rückkanälen, setzen Maßstäbe außerhalb der Polizeien. Verschiedene Lösungen werden bis heute für die interne Kommunikation diskutiert. Den mutigsten Schritt wagt bislang die Polizei Niedersachsen mit ihrem corporate social intranet, das neben klassischen Intranet-Informationen auch Social-Media-Funktionen einbindet und damit erstens ortsübergreifende Zusammenarbeit ermöglicht, zweitens die zahlreichen

Kompetenzen der Mitarbeitenden sichtbar machen kann sowie drittens Diskussionsforen oder Technikblogs ermöglicht. Ergänzend zur stationären Nutzung auf Dienstrechnern soll das Intranet zukünftig auch über eine App auf Smartphones verfügbar gemacht werden. Die Polizei Niedersachsen setzt hier wie auch beim eigenen Messengerdienst NiMes auf die „Bring your own device"-Strategie.

Neben diesen technischen Errungenschaften benötigen die Mitarbeitenden immer mehr spezialisierte Kompetenzen. Das moderne Kommunikationsmanagement erfordert strategisches Denken wie auch technisches Know-how.

Professionalisierung und Strategische Kommunikation

Von der fehlenden Qualifizierung der Pressestellen kann nur noch bedingt die Rede sein. Zwar erhalten Mitarbeitende nicht immer direkt zu Beginn der Verwendung in der Presse- und Öffentlichkeitsarbeit eine entsprechende Fortbildung (vgl. Jarolimek et al., 2026), aber durch das erweiterte Aufgabenspektrum ist eine zunehmende Professionalisierung sichtbar, teils durch spezialisierte Weiterbildungen, teils durch Tarifangestellte.

Die Akademisierung ist in den Kommunikationsabteilungen deutlich gestiegen (vgl. Jarolimek et al., 2026), zum einen durch die Tarifangestellten und die Abschaffung des „mittleren Dienstes" in einigen Polizeien sowie zum anderen durch die zunehmende Besetzung der Pressestellenleitung mit einem Beamten im vierten Einstiegsamt (ehemals höherer Dienst). Abbildung 3 zeigt die Entwicklung der Tarifangestellten sowie den akademischen Hintergrund.

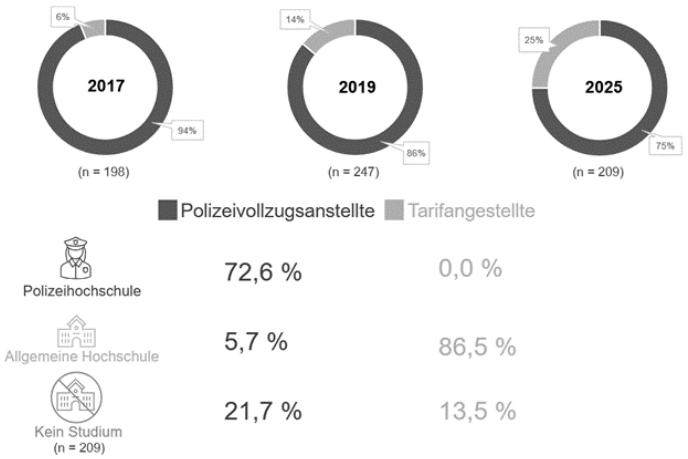


Abb. 3: Entwicklung Karriereweg (Jarolimek et al., 2026, S. 16)

Darüber hinaus existieren mehrere Weiterbildungsformate für Mitarbeitende in den Kommunikationsabteilungen, z. B. im Bereich Social Media ein einwöchiger „Grundkurs" Social Media, der vom Bundeskriminalamt durchgeführt wird, sowie die dreiwöchige, zertifizierte Weiterbildung „Social Media Manager/in Polizei", die regelmäßig von der Deutschen Hochschule der Polizei in Münster angeboten wird. Weitere Angebote für Pressestellenleiter und Mitarbeitende im Presse- und Social-Media-Bereich wären wünschenswert: Neben den veränderten Software-Anwendungen und Technologien existieren derzeit nur wenige Fortbildungen mit Blick auf weitere Kompetenzen, z. B. Interviewtraining oder Content Creator.

Meist wird die konkrete Nutzung von Softwarelösungen autodidaktisch erlernt. Abbildung 4 verdeutlicht den erheblichen Mangel an einer institutionalisierten Fort- und Weiterbildung im Bereich Presse- und Öffentlichkeitsarbeit.

Durch die Vielzahl der kommunikativen Möglichkeiten über Pressearbeit, Intranet, Internet und Social-Media-Kanäle gilt es Entscheidungen darüber zu treffen, welche Ziele und Zielgruppen mit welchen Mitteln und Botschaften erreicht werden sollen. Hierfür sind Kommunikationsstrategien nötig.

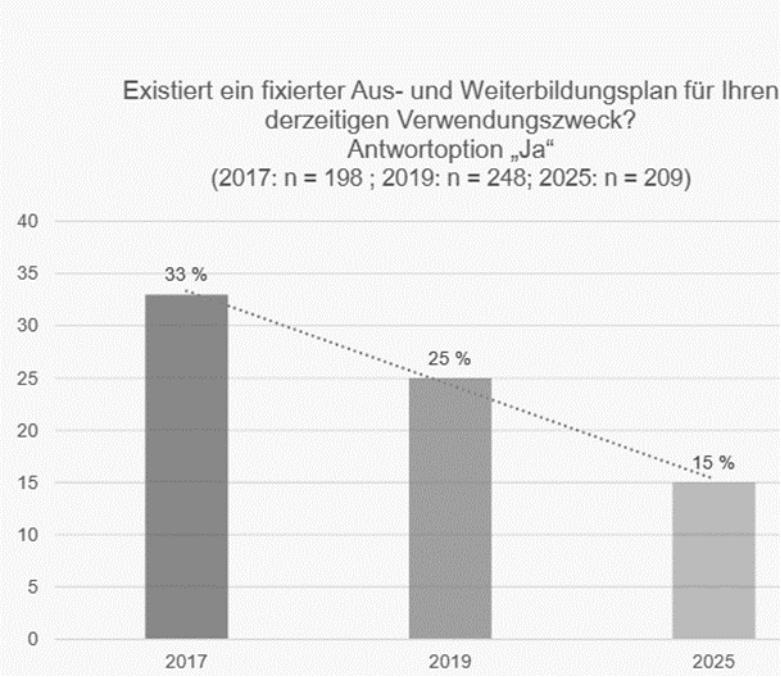
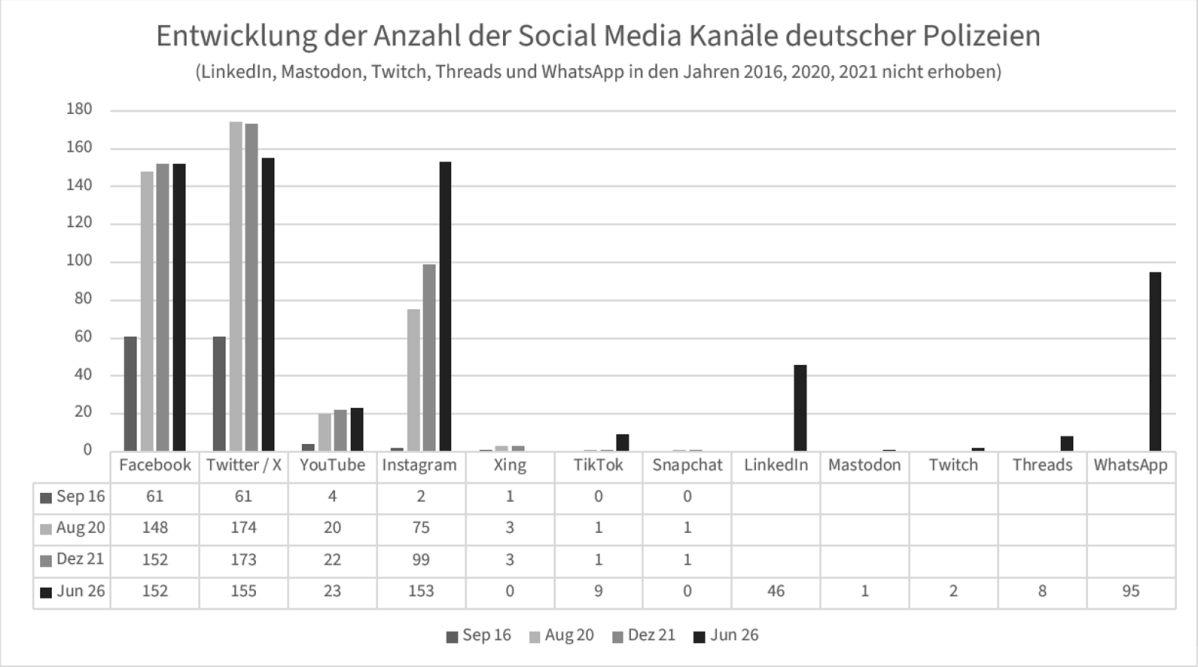


Abb. 4: Entwicklung Aus- und Weiterbildung (Jarolimek et al., 2026, S. 21)

Die seit 2016 regelmäßig durchgeführte Berufsfeldstudie *Profession Kommunikation in der Polize*i, die neben polizeispezifischen Fragen weitere Items branchenübergreifender PR-Berufsfeldstudien einbezieht (national Seidenglanz, 2025, europäisch Tench et al., 2025), zeigt diese Tendenzen. Die strategische Herangehensweise sowie medienrechtliche Fragen haben deutlich an Bedeutung gewonnen.

Dies wird umso bedeutender, da die Anzahl der Social-Media-Kanäle stetig zunimmt. Sowohl die Anzahl der individuell betriebenen Kanäle (Corporate Influencer) als auch die der Kanäle der Kommunikationsabteilungen verdeutlichen dies. Abbildung 5 zeigt die Entwicklung von 2015 bis zu den aktuellen Zahlen 2026.



	Facebook	Twitter / X	YouTube	Instagram	Xing	TikTok	Snapchat	LinkedIn	Mastodon	Twitch	Threads	WhatsApp
Sep 16	61	61	4	2	1	0	0					
Aug 20	148	174	20	75	3	1	1					
Dez 21	152	173	22	99	3	1	1					
Jun 26	152	155	23	153	0	9	0	46	1	2	8	95

Abb. 5: Entwicklung der Anzahl der Social-Media-Kanäle der deutschen Polizeien, Quelle: Stelle zur Koordinierung Soziale Medien (Niedersächsisches Ministerium für Inneres, Sport und Digitalisierung/Deutsche Hochschule der Polizei)

Aktuelle Herausforderungen: Twitch und KI

Die Entwicklung der Kanäle und Möglichkeiten geht weiter und ist mit immer neuen technologischen Anforderungen verbunden. Bereits 2018 wird beim Treffen der Social-Media-Teams der deutschen Polizeien über die Möglichkeiten von TikTok, aber auch Twitch gesprochen. Twitch ist zunächst als reine Gaming-Plattform gestartet, bei der Nutzer*innen den Spielenden zuschauen und sich im Chat austauschen können. Aus den Gesprächen mit den Gamer*innen entstehen das reine Gesprächs- und Diskussionsformat „Just Chatting“ sowie weitere Formen, z. B. IRL (In Real Life). Niedersachsen hat als erste Polizei mit dem Projekt Twitch-Team der Polizei Hannover, inzwischen Polizei Niedersachsen, den Schritt ins Gaming-Format gewagt. Twitch ermöglicht einen niedrigschwelligen Kontakt zur Zielgruppe der Jugendlichen und jungen Erwachsenen, die die Polizei sonst kaum (auch nicht über Social-Media-Kanäle) erreicht. Parallel zum Spielen oder in eigenen Just-Chatting-/IRL-Formaten werden Präventionsbotschaften vermittelt, die Polizei vorgestellt oder Einsätze erläutert. Neben ethischen und medienrechtlichen Herausforderungen (Stichworte sind hier Gewaltspiele und staatlicher Rundfunk) und internen Diskussionen („Spielen im Dienst“) benötigte das Twitch-Team eine neue, andere medientechnische Ausstattung. Beschafft werden mussten Studio, mehrere Kameras, Gaming-PCs, Spiele usw. Abb. 6 vermittelt einen Eindruck des Twitch-Studios, das nur wenig mit der früheren Amtsstube gemein hat.

Abb. 6: Studio des Twitch-Teams der Polizei Niedersachsen (Quelle: Instagram Polizei Hannover)

Daneben erfährt Künstliche Intelligenz seit zwei bis drei Jahren eine große Aufmerksamkeit in der Presse- und Öffentlichkeitsarbeit. Im Mittelpunkt stehen die Fragen, wie, wozu und in welchem Umfang KI von Polizeien genutzt werden kann und darf. Wie in den Anfangsjahren von Social Media sind es zum Teil Einzelpersonen, die mit Privatlizenzen von chatGPT oder notebookLM u. a. Texte bearbeiten sowie Videos oder Podcasts erstellen. Neben (datenschutz-)rechtlichen Fragen spielen auch ethische Bewertungen eine Rolle. Wenn Kollegen bei der Pressestelle anrufen und nachfragen, wer denn wohl die junge (KI-generierte) Kollegin im Video sei, wird deutlich, dass KI-Informationen kaum wahrgenommen werden. Einzelne Pressestellen mit eigener „Polizei-KI“ nutzen diese bereits, um aus Lageberichten Pressemitteilungen zu entwerfen.

Stand Mitte 2026 konsolidiert sich die Nutzung von KI in der Polizei, insbesondere mit Blick auf die unterschiedlichen Aufgaben, die die Polizeien als denkbar oder wünschenswert erachten. Diese betreffen neben einfacher Unterstützung zur Contenterstellung (Text, Bild, Bewegtbild) zukünftig vor allem Anwendungen für das Issues Management, etwa zur Erkennung von Desinformation oder Deepfakes.

Fazit

Die Darstellung verdeutlicht den im Vergleich zu deutschen Großunternehmen späten Einstieg der Polizeien in die institutionalisierte Presse- und Öffentlichkeitsarbeit, was jedoch nicht weiter verwunderlich ist. Die wegweisende PR-Berufsfeldstudie von Röttger (2010) aus

dem Jahr 2000 zeigt, dass auch bei kleineren und mittleren Unternehmen die Pressearbeit noch um die Jahrtausendwende von der Geschäftsführung oder anderen „PR-Laien“ mit erledigt wurde.

Die changierenden Begrifflichkeiten der Aufgaben und Abteilungen in dem Berufsfeld kennzeichnen auch den vorliegenden Text: vom Nachrichtenbüro zur Pressestelle, von der Presseabteilung zu Public Relations und Öffentlichkeitsarbeit. Die Bezeichnung Presse- und Öffentlichkeitsarbeit wird meines Wissens nur in der Polizei so genutzt und unterschieden. Public Relations und Öffentlichkeitsarbeit hatten und haben begrifflich ein negatives Image, da ihnen etwas Persuasives, Manipulierendes anhaftet. Durch die Entwicklung, Verbreiterung der Aufgabenbereiche und Professionalisierung zum Kommunikationsmanagement werden jene Abteilungen in anderen Organisationen häufig schlicht Kommunikation genannt. Innerhalb der Polizei sind derzeit ebenfalls Tendenzen zu einer entsprechenden Umbenennung erkennbar, allerdings noch sehr verhalten.

Der historische Abriss seit den 1950er Jahren verdeutlicht, wie die Pressestellen erst mit Telefon und Brief arbeiteten, dann zwanzig Jahre später mit dem Faxgerät eine erste Erweiterung erfuhren. Das Internet sorgte in den 1990er Jahren für einen ersten technischen Schub. Der technologische Boom setzte in der Presse- und Öffentlichkeitsarbeit in den 2010er Jahren ein. Internet, Intranet und Social Media beschleunigen die (öffentliche und interne) Kommunikation. Diese Möglichkeiten führen zu einem enormen Zuwachs an Technik und Technologien, sowohl in der Hard- als auch in der Software. Künftige Entwicklungen (u. a. Twitch und KI) werden diesen Trend zusätzlich anheizen. Gleichwohl bleibt gerade in der Pressestelle das Telefon zentrales Medium.

Referenzen

Bentele, G. (1997). PR-Historiographie und funktional-integrative Schichtung. Ein neuer Ansatz zur PR-Geschichtsschreibung. In P. Szyszka (Hrsg.), Auf der Suche nach Identität – PR-Geschichte als Theoriebaustein (S. 137–169). Vistas Verlag.

Bentele, G. (2013). Der Diskurs über PR-Geschichte und PR-Historiographie in Deutschland und international. In O. Hoffjann & S. Huck-Sandhu (Hrsg.), UnVergessene Diskurse – 20 Jahre PR- und Organisationskommunikationsfor-schung (S. 197–235). Springer VS (Wiesbaden).

Erler, T. (2020). Der Corporate-Newsroom als Modell für die strategische Kommunikation der Polizei. Deutsche Hochschule der Polizei (unveröffentlichte Masterarbeit).

Graßl, M. (2023). Polizeikommunikation auf Social Media. Ziele, Strategien, Inhalte. Springer.

Hundhausen, C. (1951). Werbung um öffentliches Vertrauen. Public Relations. Girardet.

Jarolimek, S. (2020). Smartphones in Police Operations: The Necessity of Media Literacy in Police Forces in the Age of Transparency. European Journal for Security Research, 5, 105–114.

Jarolimek, S., & Böhmer, M. (2017). Kommunikation als Profession. Das Berufsfeld Presse- und Öffentlichkeitsarbeit in der Polizei 2016. Deutsche Hochschule der Polizei Hochschulverlag.

Jarolimek, S., Marpe, K. S., & Melzer, A. (2025). Kommunikation als Profession. Das Berufsfeld Presse- und Öffentlichkeitsarbeit in der Polizei 2025. Deutsche Hochschule der Polizei Hochschulverlag.

Jarolimek, S., Rittig, S., Stumpen, H. A., & Tamborini, Y. (2023). Polizei und Social Media. Rechtliche Grundlagen, Öffentlichkeitsarbeit und private Nutzung. Boorberg.

Kunczik, M. (2009). PR-Theorie und PR-Praxis. Historische Aspekte. In G. Bentele, R. Fröhlich & P. Szyszka (Hrsg.), Handbuch der Public Relations. Wissenschaftliche Grundlagen und berufliches Handeln. Mit Lexikon (S. 223−239). 2., korrigierte und erweiterte Auflage. VS.

Kunz, M. (2018). Die Professionalisierung der Organisationskommunikation am Beispiel der Polizei Rheinland-Pfalz. Deutsche Hochschule der Polizei (unveröffentlichte Masterarbeit).

Kutsch, A., Sterling, F., & Fröhlich, R. (2011). Korrespondenzen im Deutschen Kaiserreich und in der Weimarer Republik. Rekonstruktion und sekundärstatistische Analyse eines medialen Sektors. Jahrbuch für Kommunikationsgeschichte, 13, 154−176.

Moss, C. (2022). Corporate Newsroom. Gabal.

Oeckl, A. (1987). Anfänge der Öffentlichkeitsarbeit. PR-Magazin, 18(2), 23−30.

Röttger, U. (2010). Public Relations – Organisation und Profession. Öffentlichkeitsarbeit als Organisationsfunktion. Eine Berufsfeldstudie. 2. Auflage. VS.

Seidenglanz, R. (2024). Profession Kommunikation. Die Berufsfeldstudie 2024. Quadriga Media.

Sadrowski, M., & Jarolimek, S. (2016). Corporate Newsroom. Eine neue Organisationsform für die Unternehmenskommunikation. The Reporting Times, 9, 26.

Szyska, P. (1990). Der Mythos vom „anderen“ Journalisten. Ein Berufsbild zwischen Schein und Sein. PR-Journal, 21(4), 27-38.

Tench, R., Moreno, A., Romenti, S., Buhmann, A., Laborde, A., & Zerfass, A. (2025). European Communication Monitor 2025/26. Intergenerational challenges in corporate communications: Exploring corporate positioning, talent management and coaching. European Public Relations Education and Research Association (EUPRERA).

Digitale Forensik nach Ernst Gennat – Methodisches Denken im Zeitalter digitaler Spuren

Dirk Labudde und Roman Povalej

Die fortschreitende Digitalisierung verändert die kriminalistische Ermittlungsarbeit grundlegend und stellt Polizeibehörden vor neue methodische, technische und rechtliche Herausforderungen. Der vorliegende Beitrag verbindet die kriminalistische Systematik Ernst Gennats (1880–1939) mit den Anforderungen moderner digitaler Forensik (Labudde & Spranger, 2017; Fähndrich et al., 2023). Aufbauend auf einer historischen und epistemologischen Einordnung seiner praxisbasierten Methodik werden Dual-Use-Technologien, der kriminalistische Innovationszyklus sowie aktuelle Entwicklungen der Polizeitechnik analysiert. Tabellen und Fallbeispiele verdeutlichen die Übertragbarkeit klassischer kriminalistischer Prinzipien auf digitale Ermittlungsumgebungen. Der Beitrag zeigt, dass Gennats Ansatz eine zeitlose Grundlage für datengetriebene, simulationsbasierte und interdisziplinäre Polizeiarbeit im 21. Jahrhundert darstellt und eine Brücke zwischen analoger Kriminalistik und digitaler Forensik bildet.

Die Digitalisierung hat die Polizeiarbeit in den vergangenen Jahrzehnten tiefgreifend transformiert. Kriminalität manifestiert sich zunehmend im digitalen Raum, während gleichzeitig klassische Deliktsformen durch Nutzung neuer digitaler Technologien für Begehensweisen erweitert oder ersetzt werden. Diese Entwicklung erfordert nicht nur neue technische Kompetenzen, sondern auch ein erneuertes methodisches Verständnis kriminalistischer Erkenntnisprozesse. In diesem Kontext bietet das Werk des Berliner Kriminalisten Ernst Gennat eine bemerkenswert aktuelle Perspektive. Seine praxisbasierte Systematik stellt ein zeitloses Modell dar, das sich auf die Herausforderungen der digitalen Forensik übertragen lässt.

Ernst Gennat und die Entstehung kriminalistischer Systematik aus der Praxis – Eine epistemologische Einordnung

Praxis als Erkenntnisquelle der Kriminalistik

Die Entwicklung kriminalistischer Methodik ist historisch weniger das Ergebnis theoretischer Vorüberlegungen als vielmehr das Produkt praktischer Notwendigkeiten. In diesem Sinne stellt Ernst Gennat, langjähriger Leiter der Zentralen Mordinspektion (ZMI) am Berliner Alexanderplatz (auf sein Drängen hin 1926 gegründet), eine Schlüsselfigur der epistemischen Transformation polizeilicher Ermittlungsarbeit dar. Seine Reformen markieren den Übergang von einer erfahrungsgeleiteten, individualisierten Ermittlungsweise hin zu einer systematisch strukturierten, evidenzbasierten und institutionell verankerten Kriminalistik.

Gennats Bedeutung liegt nicht allein in organisatorischen Innovationen oder spektakulären Fahndungserfolgen, sondern in der Entwicklung einer kriminalistischen Erkenntnisordnung, die aus der Praxis erwuchs und zugleich theoretische Implikationen für die moderne Polizeiarbeit besitzt. Seine Arbeit kann als frühe Form einer praxeologischen Epistemologie verstanden werden, in der Wissen durch wiederholte Handlung, strukturierte Dokumentation und vergleichende Analyse generiert wird.

Historischer Kontext: Urbanität, Komplexität und Professionalisierung

Die ersten Jahrzehnte des 20. Jahrhunderts waren durch tiefgreifende gesellschaftliche Transformationsprozesse geprägt. Berlin entwickelte sich zu einer hochkomplexen Metropole mit steigender Bevölkerungsdichte, sozialer Mobilität und zunehmender Anonymität. Diese Urbanisierung führte zu neuen Erscheinungsformen der Kriminalität, insbesondere zu komplexen Tötungsdelikten und Serienverbrechen, die traditionelle Ermittlungsansätze überforderten.

Die Kriminalpolizei befand sich zu dieser Zeit in einem Spannungsfeld zwischen bürokratischer Institutionalisierung und fehlender methodischer Standardisierung. Ermittlungen waren häufig personenbezogen organisiert, Wissen wurde nicht systematisch archiviert, und vergleichende Fallanalysen waren kaum etabliert. In diesem Kontext entwickelte Gennat seine Reformen, die als Antwort auf die wachsende Komplexität urbaner Kriminalität verstanden werden können.

Organisationsreform als epistemische Innovation

Mit der Übernahme der Leitung der ZMI Berlin etablierte Gennat eine organisatorische Spezialisierung, die weit über administrative Effizienz hinausging. Die Schaffung einer dauerhaft zuständigen Einheit für Tötungsdelikte ermöglichte erstmals die Akkumulation kollektiven Ermittlungswissens und die Entwicklung standardisierter Arbeitsprozesse.

Diese Zentralisierung führte zu einer Verschiebung des Erkenntnisparadigmas: Wissen wurde nicht mehr ausschließlich als individuelles Erfahrungswissen einzelner Ermittler verstanden, sondern als institutionell gespeicherte und kollektiv nutzbare Ressource. Die systematische Archivierung von Fallakten und die vergleichende Analyse von Tatmustern schufen die Grundlage für eine strukturierte kriminalistische Wissensproduktion. Damit antizipierte Gennat zentrale Prinzipien moderner datenbasierter Ermittlungsstrategien.

Der Tatort als Zentrum der Erkenntnisgewinnung

Ein zentrales Element von Gennats kriminalistischer Systematik war die konsequente Tatortzentrierung. Der Tatort wurde nicht länger als bloßer Ausgangspunkt der Ermittlungen betrachtet, sondern als primäres epistemisches Objekt, aus dem kriminalistische Erkenntnis generiert wird.

Durch die Einführung standardisierter Tatortprotokolle, die strikte Trennung von Spurensicherung und Vernehmung sowie die konsequente Dokumentation aller Befunde etablierte Gennat eine methodische Ordnung, die kognitive Verzerrungen minimieren und die Reproduzierbarkeit kriminalistischer Analysen gewährleisten sollte. Diese Herangehensweise kann als frühe Form evidenzbasierter Ermittlungsarbeit interpretiert werden.

Technologische Praxisinnovation: „Das Mordauto“

Die Einführung des sogenannten „Mordautos“ stellt ein paradigmatisches Beispiel für die aus der Praxis erwachsene Systematik dar. Dieses speziell ausgestattete Einsatzfahrzeug ermöglichte eine standardisierte und sofortige Spurensicherung direkt am Tatort. Die mobile Bereitstellung kriminaltechnischer Ausrüstung reduzierte improvisatorische Elemente und erhöhte die methodische Qualität der Tatortarbeit.

Epistemologisch betrachtet fungierte das „Mordauto“ als infrastrukturelle Erweiterung des Tatortes: Es schuf die materiellen Voraussetzungen für eine systematische Datenerhebung und kann somit als Vorläufer moderner mobiler forensischer Labore verstanden werden. In der heutigen Polizeitechnik findet dieses Prinzip seine Fortsetzung in hochspezialisierten Tatortfahrzeugen und digitalen Cyber-Lab-Einheiten.

Mustererkennung und die Genese kriminalistischer Analyseverfahren

Gennats Arbeit zeichnete sich durch ein ausgeprägtes Verständnis für die Bedeutung von Mustern und Wiederholungstatbeständen aus. Durch die systematische Vergleichsanalyse von Tatorten, Täterverhalten und Opferprofilen entwickelte er eine methodische Grundlage, die späteren Profiling-Ansätzen vorausging.

Die häufig zitierte Einführung des Begriffs „Serienmörder“ im Zusammenhang mit den Düsseldorfer Sexualverbrechen unterstreicht seine analytische Perspektive. Entscheidend war hierbei nicht die terminologische Innovation, sondern die Etablierung eines strukturierten Vergleichsverfahrens, das kriminalistische Hypothesen auf empirische Daten stützte. Diese Form der Mustererkennung stellt eine frühe Ausprägung datenbasierter Kriminalistik dar.

Öffentlichkeit als epistemische Ressource

Ein weiterer innovativer Aspekt von Gennats Arbeit war der strategische Umgang mit der Presse. Während Öffentlichkeit traditionell als Risiko für Ermittlungen betrachtet wurde, erkannte Gennat ihr Potenzial als Quelle der Informations- und Erkenntnisgewinnung. Durch gezielte Informationssteuerung konnte die Bevölkerung in Fahndungsprozesse eingebunden und gleichzeitig die Legitimation polizeilicher Arbeit gestärkt werden.

Diese Kommunikationsstrategie reflektiert ein erweitertes Verständnis kriminalistischer Erkenntnisproduktion, in dem Wissen nicht ausschließlich innerhalb der Institution Polizei entsteht, sondern auch durch Interaktion mit der Gesellschaft generiert wird.

Praxeologische Epistemologie der Kriminalistik

Die kriminalistische Systematik Gennats lässt sich als praxeologische Epistemologie beschreiben: Wissen entsteht durch wiederholte Handlung, strukturierte Dokumentation und institutionelle Speicherung. Theorie ist hierbei nicht Ausgangspunkt, sondern Resultat praktischer Erfahrung.

Diese Erkenntnisordnung weist bemerkenswerte Parallelen zu modernen datengetriebenen Ermittlungsansätzen auf. Der digitale Zwilling des Tatortes, relationale Evidenzdatenbanken und simulationsbasierte Hypothesenprüfungen folgen derselben Logik: Kriminalistische Erkenntnis wird durch strukturierte Datenerhebung, Vergleichbarkeit und iterative Analyse generiert. Jedoch darf kriminalistische Erkenntnis nicht im Einzelfall stecken bleiben, sondern erfordert ein theoretisch abgeleitetes, umspannendes Konstrukt.

Bedeutung für die moderne Polizeitechnik

Die strukturelle Kontinuität zwischen Gennats Systematik und aktuellen Entwicklungen der Polizeitechnik ist evident. Während Gennat mit analogen Mitteln arbeitete, verfolgen moderne Systeme – etwa digitale Zwillinge oder das Konzept des Forensiums (Labudde, 2026) – denselben Ansatz der Erkenntnisgewinnung: den Tatort als datenbasiertes Informationssystem zu verstehen und kriminalistische Hypothesen modellgestützt zu prüfen.

Gennats Arbeit kann somit als historischer Referenzpunkt einer Entwicklungslinie betrachtet werden, die von der standardisierten Tatortarbeit über kriminalstatistische Analysen bis hin zu simulationsbasierten digitalen Ermittlungsumgebungen reicht. Seine praxisbasierte Systematik bildet die epistemische Grundlage moderner, technologisch unterstützter Kriminalistik.

Der Rückblick auf Ernst Gennat verdeutlicht, dass die Professionalisierung der Kriminalpolizei nicht primär durch technologische Innovationen, sondern durch die Entwicklung einer strukturierten Erkenntnisordnung vorangetrieben wurde. Gennats aus der Praxis erwachsene Systematik transformierte kriminalistische Ermittlungsarbeit nachhaltig und etablierte Prinzipien, die bis heute Gültigkeit besitzen: Tatortzentrierung, Standardisierung, institutionelle Wissensspeicherung und hypothesengeleitete Analyse.

In einer Zeit, in der digitale Technologien die Polizeiarbeit zunehmend prägen, bleibt Gennats Ansatz von hoher Aktualität. Er zeigt, dass nachhaltige Innovation in der Kriminalistik nicht allein auf technischem Fortschritt beruht, sondern auf der methodischen Integration von Erfahrung, Struktur und Erkenntnis. Damit ist Ernst Gennat nicht nur eine historische Figur, sondern ein epistemologischer Wegbereiter moderner kriminalistischer Systemarchitekturen.

Vom „Mordauto“ zum Cybermobil

Die kriminalistische Systematik Ernst Gennats zeigt exemplarisch, wie Innovationen in der Polizeiarbeit aus praktischen Erfordernissen entstehen und sich in nachhaltigen organisatorischen sowie methodischen Strukturen verfestigen. Mit dem „Mordauto“ schuf Gennat nicht nur ein technisches Hilfsmittel, sondern ein mobiles Einsatzkonzept, das die Tatortarbeit standardisierte, beschleunigte und qualitativ verbesserte. Dieses Fahrzeug verkörperte bereits in den 1920er Jahren den Anspruch, kriminaltechnische Expertise unmittelbar am Ereignisort verfügbar zu machen und Ermittlungen evidenzbasiert zu strukturieren.

Aus epistemologischer Perspektive markiert das „Mordauto“ den Beginn einer Entwicklung, in der Mobilität, Technologie und kriminalistische Systematik zu einem integrierten Handlungskonzept verschmelzen. Die Idee, den Tatort durch technische Infrastruktur zu erwei-

tern und Wissen systematisch zu generieren, findet in der modernen Polizeitechnik ihre konsequente Fortsetzung. Während Gennats Ansatz noch auf analogen Instrumenten beruhte, operieren heutige Ermittlungsbehörden mit digitalen, vernetzten und hochautomatisierten Systemen, die den Tatort nicht nur dokumentieren, sondern als datengetriebenen Analyse- und Simulationsraum nutzbar machen.

Vor diesem Hintergrund lässt sich eine direkte Entwicklungslinie vom historischen „Mordauto“ zum modernen Cybermobil der Polizei ziehen. Das Cybermobil steht sinnbildlich für die Transformation kriminaltechnischer Mobilität im Zeitalter der Digitalisierung: Es vereint mobile Forensik, digitale Spurensicherung, Echtzeit-Datenanalyse, vernetzte Kommunikation und immersive Visualisierungstechnologien in einer integrierten Plattform. Damit wird die von Gennat begründete Idee eines mobilen kriminalistischen Kompetenzzentrums in eine neue technologische Dimension überführt.

Die folgende Betrachtung zeichnet diese Entwicklung nach und zeigt, wie sich das kriminalistische Leitprinzip der praxisbasierten Systematik – von der analogen Tatortarbeit bis hin zu cyber-physischen Einsatzsystemen – kontinuierlich weiterentwickelt hat. „Vom Mordauto zum Cybermobil“ beschreibt somit nicht nur einen technologischen Fortschritt, sondern eine epistemische Kontinuität kriminalistischer Innovation.

Technologische Transformation der Forensik im Spiegel der „Gennat’schen Denkfigur“

Die Entwicklung forensischer Technologien seit den 1990er Jahren lässt sich nicht nur als Abfolge technischer Innovationen beschreiben, sondern auch als Ausdruck eines tieferliegenden Wandels kriminalistischer Erkenntnispraktiken. Die hier dargestellte Zeitleiste kann dabei produktiv im Sinne einer „Gennat’schen Denkfigur“ interpretiert werden – also unter Rückgriff auf die von Ernst Gennat aus der Praxis geprägte Vorstellung der Kriminalistik als systematische, interdisziplinäre und hypothesengeleitete Ermittlungswissenschaft.

Gennat verstand Kriminalistik nicht primär als Sammlung von Methoden, sondern als strukturierte Denkweise, die auf der Verbindung von Beobachtung, Vergleich und Rekonstruktion basiert. Überträgt man dieses Verständnis auf die technologische Entwicklung der letzten Jahrzehnte, so wird deutlich, dass jede neue Technologie vor allem eine Erweiterung kriminalistischer Denk- und Handlungsmöglichkeiten darstellt.

Mit der Einführung von AFIS in den frühen 1990er Jahren beginnt eine Phase der Digitalisierung klassischer Identifikationsverfahren. Aus der Perspektive Gennats wäre dies weniger als bloße Effizienzsteigerung zu verstehen, sondern als Transformation des Vergleichsprinzips: Der Fingerabdruck wird von einem lokal gebundenen Beweismittel zu einem jederzeit abrufbaren Element in einem vernetzten Erkenntnissystem. Die hypothetische Adaption eines dezentralen Zugriffs für Streifenbeamte entspricht dabei der konsequenten Ausweitung des kriminalistischen Denkraums in den operativen Alltag.

Die Etablierung von DNA-Datenbanken in den späten 1990er Jahren markiert eine weitere Verdichtung dieses Systems. Die DNA fungiert als hochpräziser Identifikator und erweitert das Spektrum kriminalistischer Beweisführung erheblich. Aus einer Gennat’schen Perspekti-

ve wäre hier insbesondere die Verschiebung von der reinen Spurensicherung hin zur unmittelbaren Interpretation von Bedeutung. Mobile DNA-Kits am Tatort würden diese Entwicklung radikalisieren, indem sie die zeitliche Trennung von Spurenerhebung und Analyse aufheben.

Mit der Möglichkeit mobiler forensischer Werkzeuge um das Jahr 2000 verschiebt sich der Fokus der Kriminalistik erneut. Digitale Geräte werden zu zentralen Trägern relevanter Informationen. In diesem Kontext gewinnt das Prinzip der situativen Analyse an Bedeutung: Erkenntnisse müssen nicht nur gewonnen, sondern in Echtzeit in den Ermittlungsprozess integriert werden. Die Smartphone-Analyse vor Ort entspricht somit einer Beschleunigung kriminalistischer Zirkularität – dem ständigen Wechsel zwischen Hypothesenbildung und Überprüfung.

Der Übergang zur Massendatenanalyse ab etwa 2010 stellt einen qualitativen Bruch dar. Die schiere Menge verfügbarer Daten übersteigt die kognitiven Kapazitäten einzelner Ermittler. Die Integration von Data Scientists in kriminalistische Prozesse kann daher als notwendige Erweiterung der klassischen Ermittlungslogik verstanden werden. In Gennats Sinne handelt es sich hierbei nicht um eine Ablösung des Ermittlers, sondern um eine funktionale Differenzierung innerhalb des kriminalistischen Systems. Die Kunst des Kombinierens wird auf mehrere Akteure und Werkzeuge verteilt.

Mit dem Einsatz Künstlicher Intelligenz (KI) und fortgeschrittener Kryptoanalyse seit den 2020er Jahren erreicht diese Entwicklung eine neue Stufe. KI-Systeme sind in der Lage, Muster in hochdimensionalen Datenräumen zu erkennen, die dem menschlichen Zugriff weitgehend entzogen sind. Gleichzeitig verschiebt sich die Rolle des Ermittlers: von der primären Analyse hin zur Bewertung und Kontextualisierung algorithmisch generierter Ergebnisse. Die „Gennat'sche Denkfigur" fordert hier eine kritische Reflexion dieser Prozesse, da die Nachvollziehbarkeit und gerichtliche Verwertbarkeit algorithmischer Entscheidungen zentrale Herausforderungen darstellen.

Die Einführung forensischer digitaler Zwillinge ab Mitte der 2020er Jahre kann als konsequente Weiterentwicklung des kriminalistischen Rekonstruktionsprinzips interpretiert werden. Bereits Gennat betonte die Bedeutung der Tatortanalyse als Kern kriminalistischer Arbeit. Virtuelle Tatortrekonstruktionen erweitern dieses Prinzip, indem sie eine iterative und interaktive Überprüfung von Hypothesen ermöglichen. Der Tatort wird nicht mehr nur dokumentiert, sondern als dynamisches Modell verstanden, in dem unterschiedliche Szenarien simuliert werden können.

Mit dem Ausblick auf Quantencomputing (Fähndrich et al., 2025) und kryptografische Spurensicherung wird schließlich eine zukünftige Dimension sichtbar, in der sich die Kriminalistik zunehmend in hochkomplexen, mathematisch geprägten Räumen bewegt. Die Analyse verschlüsselter Daten stellt eine neue Form der Spurensuche dar, die klassische physische und digitale Grenzen überschreitet. In dieser Perspektive wird die Kriminalistik zu einer Wissenschaft, die nicht nur materielle, sondern auch abstrakte Spuren interpretiert.

In der Gesamtschau zeigt sich, dass die technologische Entwicklung der Forensik eng mit einer Transformation kriminalistischer Rationalität verbunden ist. Die „Gennat'sche Denkfigur" ermöglicht es, diese Entwicklung nicht als linearen Fortschritt, sondern als Erweite-

rung eines Erkenntnissystems zu verstehen. Zentrale Prinzipien – Vergleich, Rekonstruktion, Hypothesenbildung – bleiben bestehen, werden jedoch durch neue Technologien in ihrer Reichweite und Komplexität erheblich gesteigert.

Die Herausforderung der Zukunft liegt daher weniger in der Verfügbarkeit neuer Technologien als in deren Integration in eine kohärente kriminalistische Methodik. In diesem Sinne bleibt Gennats Ansatz hochaktuell: Die Qualität der Ermittlungsarbeit entscheidet sich nicht an der Technik allein, sondern an der Fähigkeit, diese in einen strukturierten Denkprozess einzubetten.

Abb. 1: Ausgewählte Meilensteine für die Polizeiarbeit (mit KI generiert)

Die in dieser Abbildung dargestellte Entwicklung verdeutlicht eine fundamentale Dynamik. Gennats überragende Stärke war es stets, kriminelle Logik zu antizipieren, bevor sie zum gesellschaftlichen Massenphänomen wurde. Während der „Tote Briefkasten" früher ein exklusives Werkzeug der Spionage und Unterwelt war, ist durch diese rasante Evolution heute jede moderne App ein potenzieller Tatort mit Dual-Use-Charakter (Nutzen vs. Missbrauch).

Dieser Perspektivwechsel ist zwingend nötig, weil die Digitalisierung die Hemmschwelle zur Delinquenz dramatisch senkt. Früher brauchte ein Täter zwingend physische kriminelle Kontakte – für Waffen, Gift, Pässe. Heute reicht ein App-Store-Account. Wir müssen uns daher von der Annahme „Es ist nur eine App" lösen und zu der Prämisse „Es ist ein Tatmittel mit globaler Reichweite" gelangen.

Was würde also Gennat tun?

Digitalisierung und Dual-Use

Um die soeben aufgeworfene Frage zu beantworten: Ernst Gennat würde die Kriminalistik radikal an die veränderten Aggregatzustände der digitalen Welt anpassen. Die retrospektive Betrachtung der forensischen Evolution zeigt nämlich, dass die Digitalisierung meist keine völlig neuen menschlichen Bedürfnisse erschafft, sondern bestehende Prozesse der Kriminalität und ihrer Bekämpfung radikal beschleunigt, skaliert oder automatisiert. Wir haben uns unaufhaltsam von der physischen Materie (Papier, Münze, Körper) hin zur reinen Information (Bit, Hash, Signal) bewegt. Angewandt auf Gennats historische Methodik bedeutet

dies: Er müsste heute kein „klassisches Mordauto“ mehr an den Tatort schicken, sondern einen hochmodernen „Incident Response Truck“, der flüchtige Server-Abbilder sichert und digitale Spuren im Moment des ersten Zugriffs unmanipulierbar konserviert.

Transformation kriminalistischer Wirklichkeit

Digitale Technologien haben die Natur kriminalistischer Spuren grundlegend verändert. Während klassische Tatorte physische Spuren aufweisen, entstehen heute digitale Tatorte, die aus Daten, Metadaten und Netzwerkinteraktionen bestehen (Povalej et al., 2021). Das Locard’sche Austauschprinzip (Locard, 1930) bleibt jedoch gültig: Jede digitale Interaktion hinterlässt unweigerlich eine Spur.

Viele moderne Technologien besitzen dabei einen inhärenten Dual-Use-Charakter (siehe auch European Union, 2021). Sie wurden für legitime Zwecke entwickelt, erweitern jedoch gleichzeitig die Handlungsmöglichkeiten von Tätern und missbrauchsanfälligen Strukturen massiv. Prominente Beispiele hierfür sind verschlüsselte Kommunikationsdienste, Kryptowährungen, Künstliche Intelligenz, Drohnentechnologie sowie das Internet der Dinge (IoT). Diese Innovationen stellen zweifellos große gesellschaftliche Errungenschaften dar, konfrontieren die Ermittlungsbehörden jedoch mit völlig neuen asymmetrischen Herausforderungen.

Aus dieser technologischen Asymmetrie entsteht eine dynamische Wechselwirkung zwischen den Akteuren des Sicherheitsraums. Das folgende relationale Modell verdeutlicht, wie diese Dynamik das Dual-Use-Dilemma von einer bloßen Bedrohung in einen direkten Motor für wissenschaftlich fundierte Fortschritte verwandelt.

Das Dual-Use-Dilemma als Treiber wissenschaftlich fundierter Innovation

Der eigentliche Motor für die Weiterentwicklung der polizeilichen Ermittlungsarbeit ist das Dual-Use-Dilemma neuer Technologien. Da jede technische Neuerung sowohl einen Nutzen als auch ein Missbrauchspotenzial besitzt, verändern sich kriminelle Handlungen fortlaufend. Täter nutzen diese Werkzeuge gezielt, um neuartige Angriffe auf die Bürger zu entwickeln. Die Bürger wiederum nutzen die Technologien im Alltag positiv, werden durch den täterseitigen Missbrauch jedoch unvorbereitet zu potenziellen Opfern.

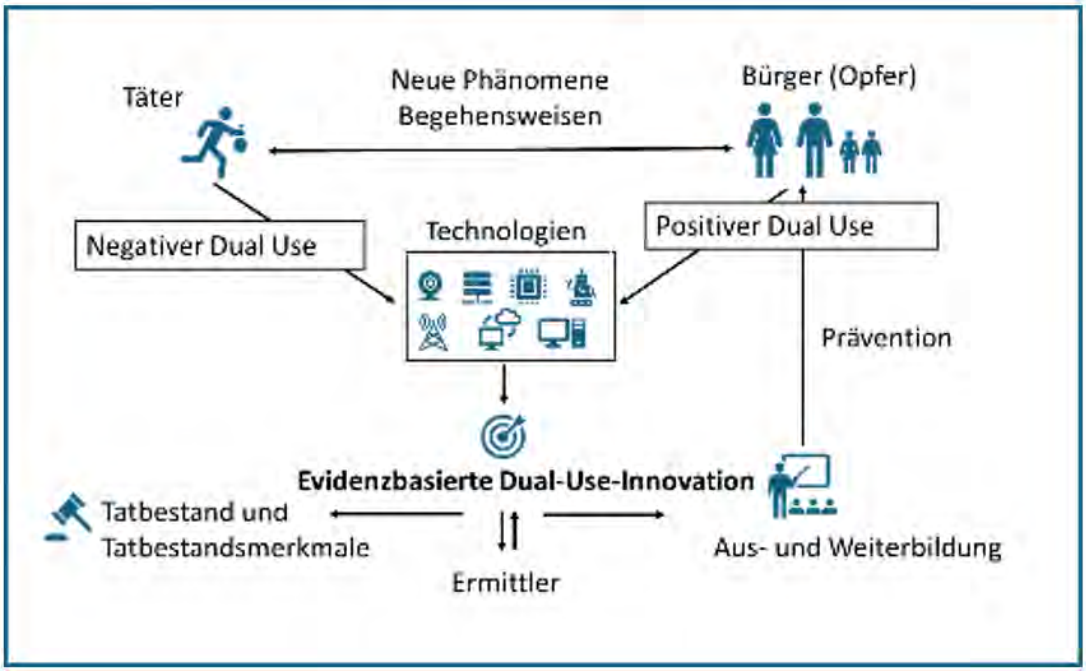


Abb. 2: Dual-Use als Innovationskatalysator für moderne Ermittlungen (angelehnt an Honekamp et al., 2023)

An dieser Schnittstelle setzt die Arbeit der Ermittler an: Sie erfassen die veränderten Angriffe und nehmen die neuartigen Tatbestandsmerkmale methodisch auf. Während Ernst Gennat diese strukturelle Erfassung seinerzeit noch rein aus der polizeilichen Praxis heraus entwickelte, ist für moderne Ermittler heute ein rein praxisgetriebenes Handeln unzureichend. Um auf die rasanten technologischen Herausforderungen der Gegenwart überhaupt vorbereitet zu sein und zukünftige Phänomene antizipieren zu können, muss Kriminalistik heute zwingend **wissenschaftlich fundiert** agieren.

Diese Symbiose aus Praxis und Wissenschaft treibt die Ermittler zu einer neuen Stufe der Innovation. Die Strafverfolgung wird dadurch befähigt, eigene technologische, methodische und theoretische Werkzeuge zu entwickeln, um moderne Delikte aufzuklären oder im besten Fall proaktiv zu verhindern. Dieses wissenschaftlich fundierte Innovationswissen bleibt jedoch nicht bei den Behörden. Es fließt in Form von Prävention und fundierten Schulungen direkt zurück an die Bürger. Auf diese Weise schließt sich der Kreis: Die Bürger lernen die Risiken der von ihnen genutzten Technologien kennen, wodurch kriminelle Angriffe bereits im Vorfeld blockiert werden.

Der kriminalistische Innovationszyklus

Die Kriminalitätsbekämpfung ist durch ein kontinuierliches Wechselspiel zwischen Tätern und Ermittlern geprägt. Jede technologische Innovation auf der einen Seite erzwingt unmittelbare Anpassungsstrategien auf der anderen Seite. Im digitalen Zeitalter hat sich dieser Zyklus erheblich beschleunigt. Um in dieser Dynamik nicht bloß reaktiv zu agieren, ist die wissenschaftliche Fundierung der Kriminalistik unumgänglich: Proaktive Strategien, wie ein polizeiliches Technologie-Radar, gewinnen dadurch existenzielle Bedeutung für eine zukunftsorientierte Gefahrenabwehr und Strafverfolgung.

Abb. 3: Fortwährender Wettlauf zwischen Ermittlungsbehörden und Kriminellen

Die technologische Evolution macht dieses asymmetrische Ringen im virtuellen Raum unmissverständlich sichtbar. Ermittlungsbehörden agieren traditionell in einem rein reaktiven Rhythmus: Ein neues technologisches Phänomen etabliert sich im Alltag, wird von kriminellen Ak-teuren adaptiert, und erst nach einer spürbaren Latenzzeit antwortet die Kriminalistik mit neuen forensischen Methoden. Um mit der rasanten Dynamik des digitalen Raums Schritt zu halten, ist die Implementierung eines polizeilichen Technologie-Radars unverzichtbar. Es dient als strategisches Frühwarnsystem, um technologische Disruptionen bereits in ihrer Entstehungsphase auf ihr kriminalistisches Missbrauchspotenzial hin abzuklopfen.

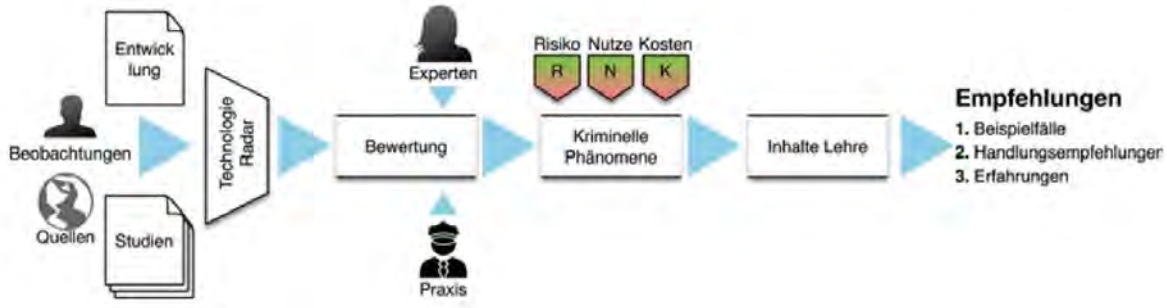


Abb. 4: Modell für die Einbringung neuer Technologien mit einem beobachtbaren Crime Potential (Honekamp et al., 2023)

Ernst Gennat hat in seiner Epoche bewiesen, dass technologischer Fortschritt nicht passiv abgewartet werden darf. Die Kernphilosophie seiner Arbeit überdauert den technischen Wandel, da seine wegweisenden Methoden direkte, digitale Entsprechungen in der modernen Cyber-Forensik finden. Dieser konzeptionelle Transfer kriminalistischer Errungenschaften verdeutlicht, dass modernes polizeiliches Handeln auf den fundamentalen Säulen des historischen Meisters aufbaut:

Historisches Konzept	Digitale Entsprechung
Mordauto	Cybermobil/Incident Response Truck
Zentralkartei	KI-gestützte Big-Data-Plattform
Tatort-Hygiene	Write-Blocker & Live-Forensik
Täterprofiling	Verhaltensbasierte Datenanalyse
Fallvergleich	Threat Intelligence

Aus dieser zwingenden Kontinuität heraus lassen sich Ernst Gennats zehn Grundregeln für die digitale Kriminalistik ableiten, die an seine unverwüstliche Ermittlungsphilosophie anknüpfen und auf die Anforderungen moderner Datenströme übertragen werden. (vgl. Labudde & Povalej, 2025):

1. **Der virtuelle Tatort ist primär:** Behandle digitale Datenströme, Protokolle und Speicherabbilder mit derselben Akribie, Systematik und Absperrdisziplin wie einen physischen Fundort.
2. **Jede Interaktion hinterlässt Spuren:** Vertraue im digitalen Raum konsequent auf das Locard'sche Prinzip; kein Löschbefehl, kein Verschlüsselungsalgorithmus und kein Anonymisierungsdienst tilgt die Spur vollständig.
3. **Antizipiere die kriminelle Logik:** Warte nicht, bis eine neue Technologie im App-Store zum Massendelikt wird, sondern analysiere und antizipiere ihr Missbrauchspotenzial ab Tag eins über ein aktives Technologie-Radar.
4. **Akzeptiere das Dual-Use-Dilemma:** Betrachte keine Alltagsanwendung und keine Komfortfunktion als inhärent harmlos; jedes smarte System ist immer auch ein potenzielles Tatmittel mit globaler Reichweite.
5. **Schütze die Integrität der Daten:** Sichere digitale Beweise im ersten Moment des behördlichen Zugriffs unmanipulierbar und kryptografisch signiert, um ihre lückenlose Kette der Beweissicherung (Chain of Custody) gerichtlich abzusichern.
6. **Nutze die Werkzeuge der Täter:** Bekämpfe Künstliche Intelligenz, Deepfakes und Krypto-Verschleierung auf Augenhöhe mit eigenen, hoch entwickelten Algorithmen, Ermittlungs-KIs und staatlicher Kryptoanalyse.
7. **Vernetze die Spezialeinheiten global:** Da digitale Kriminalität keine physischen oder nationalen Grenzen kennt, müssen Ermittlungsbehörden, Wissenschaft und Tech-Provider in standardisierten, internationalen Netzwerken kooperieren.
8. **Erstelle ganzheitliche Profile:** Verknüpfe unstrukturierte Massendaten aus Cloud-Systemen, Social Media und Streaming-Diensten, um ein präzises, datengestütztes Verhaltens- und Täterprofil zu formen.
9. **Rekonstruiere den Tatverlauf sekundengenau:** Nutze biometrische Vitaldaten aus Wearables und Protokolle aus dem Smart Home als unbestechliche digitale Zeugen, um den exakten Zeitstrahl eines Verbrechens mathematisch zu beweisen und somit präzise nachzuweisen.
10. **Bleibe dem Rechtsstaat treu:** Setze auch die mächtigsten Hochtechnologien wie Neuro-Forensik, DNA-Phänotypisierung oder orbitale Lagebildanalysen stets nur unter strikter Wahrung ethischer Standards und verfassungsmäßiger Grenzen ein.

Die Digitalisierung zwingt die Kriminalistik somit nicht dazu, ihre Grundprinzipien über Bord zu werfen, sondern sie radikal neu zu skalieren. Ernst Gennats bleibendes Vermächtnis an die moderne Strafverfolgung ist kein starres Set analoger Methoden, sondern eine geistige Haltung: die unbedingte Bereitschaft, technologische Innovationen schneller zu verstehen, zu adaptieren und zu beherrschen als die Gegenseite. Erst wenn Ermittlungsbehörden das Wechselspiel aus Dual-Use und Beschleunigung durch vorausschauende Werkzeuge wie ein aktives Technologie-Radar parieren und den Tatort mitsamt seiner Spurenlandschaft als dynamischen **digitalen Zwilling** begreifen – der weit über eine bloße Momentaufnahme hinaus das Potenzial für Echtzeit-Monitoring, kriminalistische Simulationen und hypothesenorientierte Prüfungen bietet –, wird aus der technologischen Disruption kein Kontrollverlust, sondern die logische Fortführung präziser, unbestechlicher Spurenarbeit im 21. Jahrhundert (Volkmann et al., 2025).

Zum Abschluss muss jedoch formuliert werden, dass es an der Zeit ist, die aus der polizeilichen Praxis abgeleitete Systematik Gennats auf ein wissenschaftlich-theoretisches Fundament zu stellen. Das gilt vor allem für die methodische Einbeziehung neuer Technologien im Rahmen eines hypothesengetriebenen Ermittlungsansatzes. Denn erst die theoretische Fundierung überführt die pragmatische Einzelfallanalyse in eine zukunftsfähige Kriminalistik, ganz im Sinne Georg Wilhelm Friedrich Hegels, für den feststand: **„***Die wahre Gestalt, in welcher die Wahrheit existiert, kann allein das wissenschaftliche System derselben sein***“** (Hegel, 1807/1986).

Referenzen

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Dobler, J. (2011). Ernst Gennat (1880–1939). Kriminalist, Organisator, Reformer. *Kriminalistik, 65*(2), 115–121.

European Union. (2021). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Official Journal of the European Union.

Fähndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. *Forensic Science International: Digital Investigation, 46*, Article 301617. https://doi.org/10.1016/j.fsidi.2023.301617

Fähndrich, J., Labudde, D., & Rüdiger, T.-G. (2025). Zukunft der Cyberkriminalität – drei Szenarien. *Deutsches Polizeiblatt, 2025*(6), 19–22.

Garfinkel, S. L. (2012). Lessons learned writing digital forensics tools and managing a 30 TB digital evidence corpus. *Digital Investigation, 9*(Suppl.), 80–89. https://doi.org/10.1016/j.diin.2012.05.002

Gennat, E. (1931). Die Düsseldorfer Sexualverbrechen. *Archiv für Kriminologie, 87*, 193–214.

Gennat, E. (2026). Vernehmungen – kriminalistische Strategie und Technik. *Der Kriminalist, 2026*(3–4), 11–28. https://www.bdk.de/der-bdk/was-wir-tun/publikationen/der-kriminalist/der-kriminalist-3-4-2026 (Original work published 1930).

Gross, H. (2018). *Handbuch für Untersuchungsrichter, Polizeibeamte, Gendarmen u. s. w.* (Faksimile-Nachdruck der 1. Aufl. von 1893). proLIBRIS Verlagsgesellschaft (Original work published 1893).

Gross, H. (2021). *Handbuch für Untersuchungsrichter als System der Kriminalistik: Band 1* (7., umgearb. Aufl.). De Gruyter. https://doi.org/10.1515/9783112359761 (Original work published 1922).

Hahn, N. (2026). Erinnerung an einen Wegbereiter moderner Mordermittlungen: Ernst Gennat – Pionier und Praktiker. *Der Kriminalist, 2026*(3–4), 6–10. https://www.bdk.de/der-bdk/was-wir-tun/publikationen/der-kriminalist/der-kriminalist-3-4-2026

Hegel, G. W. F. (1986). *Phänomenologie des Geistes* (Werke, Bd. 3). Suhrkamp (Original work published 1807).

Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., & Labud-de, D. (2023). Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2. Phänomene und Auswirkungen (S. 673–702). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_51

Inman, K., & Rudin, N. (2000). *Principles and practice of criminalistics: The profession of forensic science*. CRC Press.

Labudde, D. (2026). Forensium – The digital twin in forensic casework. In *Proceedings of VISUAL 2026: The Eleventh International Conference on Applications and Systems of Visual Paradigms* (Article visual_2026_1_10_70005). ThinkMind.

Labudde, D., & Mohaupt, M. (2018). *Bioinformatik im Handlungsfeld der Forensik*. Springer Spektrum.

Labudde, D., & Povalej, R. (2025). Digitale Spur und analoge Weisheit: Gennat 2.0 – Ermittlungsprinzipien im digitalen Zeitalter. *proPOLIZEI, 2025*(5), 14–15. https://polizei-nds.de/download/77499/proPolizei.Ausgabe_September_Oktober_2025.pdf.pdf

Labudde, D., & Spranger, M. (Hrsg.). (2017). *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Springer Spektrum. https://doi.org/10.1007/978-3-662-53801-2

Locard, E. (1930). *Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden* (W. Finke, Bearb.). Kameradschaft Verlagsgesellschaft (Original work published 1920).

Mohler, G. O., Short, M. B., Brantingham, P. J., Schoenberg, F. P., & Tita, G. E. (2011). Self-exciting point process modeling of crime. *Journal of the American Statistical Association, 106*(493), 100–108. https://doi.org/10.1198/jasa.2011.ap09546

Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., Honekamp, W., & Labudde, D. (2021). Die Enkel von Locard. *Informatik Spektrum, 44(5)*, 355–363. https://doi.org/10.1007/s00287-021-01393-5

Kellerhoff, S. F. (2020). *Ernst Gennat. Der „Volle Ernst“ der Berliner Kriminalpolizei*. BeBra Verlag.

Kind, S. S., & Overman, M. D. (1972). *Science against crime*. Doubleday.

Povalej, R. (2022). Cybercrime. In B. Körber, H. P. Schmalzl & M. Hermanutz (Hrsg.), *Moderne Polizeipsychologie in Schlüsselbegriffen: Ein Handbuch für die professionelle Konflikt- und Krisenbewältigung* (4. Aufl., S. 128–143). Richard Boorberg Verlag.

Raaijmakers, S. (2019). Artificial intelligence for law enforcement: Challenges and opportunities. *IEEE Security & Privacy, 17*(5), 74–77. https://doi.org/10.1109/MSEC.2019.2925640

Rademacher, T. (2020). *Artificial Intelligence and Law Enforcement.* In T. Wischmeyer & T. Rademacher (Hrsg.), *Regulating Artificial Intelligence* (S. 239–254). Springer.

Saferstein, R. (2020). *Criminalistics: An introduction to forensic science*. Pearson.

Siemens, D. (2007). *Metropole und Verbrechen: Die Gerichtsreportage in Berlin, Paris und Chicago 1919–1933*. Franz Steiner Verlag.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586

Stürickow, R. (2016). *Kommissar Gennat ermittelt: Die Erfindung der Mordinspektion* (5. Aufl.). Elsengold.

Volkmann, D., Schildein, S., Povalej, R., & Labudde, D. (2025). *Digitaler Zwilling als Schlüsseltechnologie für die Polizei: Eine kriminaltechnisch-forensische Perspektive* (Research Brief Nr. 7). IKriS – Institut für Kriminalitäts- und Sicherheitsforschung, Polizeiakademie Niedersachsen. https://www.pa.polizei-nds.de/download/77573

Wagner, P. (1996). *Volksgemeinschaft ohne Verbrecher: Konzeptionen und Praxis der Kriminalpolizei in der Weimarer Republik und des Nationalsozialismus*. Christians.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Yar, M. (2013). *Cybercrime and society*. SAGE Publications.

Automatisierung bei der Polizei – Von der Rasterfahndung über POLAS-Sammelabfragen bis zum Einsatz Künstlicher Intelligenz: vom Bürgerpolizisten zum Technikbeiwerk?

Andreas Beier

Wie verändern sich eine Polizistin oder ein Polizist im Laufe eines Berufslebens? Neben persönlichen Entwicklungen wie der Familiengründung oder persönlichen Schicksalsereignissen sind auch die Entwicklungen in der jeweiligen Polizei bzw. Polizeidienststelle relevant – und auch die gesellschaftlichen, sozialen und politischen Entwicklungen, Ereignisse und Phasen in der Bundesrepublik Deutschland haben einen wesentlichen Einfluss darauf. Die Polizei als Institution der Inneren Sicherheit hat sich im letzten halben Jahrhundert durch die Automatisierung im Dienstalltag und durch einige disruptive Änderungen bei der Polizeitechnik signifikant und nachhaltig verändert: von der Fußstreife am Ende der 1960er Jahre mit turnusmäßigen Anrufen bei der Dienststelle über spezielle Telefonapparate, die an einer Häuserwand in der Innenstadt angebracht und mit einem Schlüssel zugänglich waren, über die „Überlandfahrt“ in den 1970er Jahren mit dem kleinen VW-Käfer als Streifenwagen und der „gemischten“ (mit Mann und Frau besetzten) Streifenwagenbesatzung mit einem großen Mercedes, BMW oder Audi ab den 1990er Jahren, die neben dem üblichen Funkgerät dann auch über ein werksmäßig eingebautes Navigationssystem oder auch Moda-Geräte zur selbstständigen POLAS-Abfrage verfügten, bis hin zur Nutzung des Smartphones in den 2020er Jahren mit diversen einsatz- oder fahndungsunterstützenden Möglichkeiten, die beispielsweise während einer Einsatzfahrt vom jeweiligen Beifahrer bzw. der jeweiligen Beifahrerin im Streifenwagen genutzt werden oder auch der Unfallaufnahme dienen können, vor allem auch, um ein schnelleres Arbeiten zu ermöglichen. „Bei der Demonstration in einer Trainingshalle der Düsseldorfer Polizei (…) öffnet der Polizist seine Datenabfrage-App, scannt den Führerschein und bekommt binnen Sekunden die Rückmeldung: keine Erkenntnisse über die Fahrerin“ (vgl. Westdeutsche Zeitung): Derartiges ist im Jahr 2026 Alltag.

Und auch bei der polizeilichen Ermittlungsarbeit veränderte sich nahezu alles: von der einfachen und manuellen über die automatisierte datenbasierte Suchmethode bis hin zur Nutzung von KI-Systemen, was ebenso die Funktion und den Wesensgehalt der Polizistinnen und Polizisten in der Demokratie und in der modernen Gesellschaft der Bundesrepublik Deutschland grundlegend änderte. Daher liegt in diesem polizeihistorischen Beitrag der Fokus auf der Polizeitechnik bzw. der technischen und EDV-basierten Ausrüstung und deren Anwendung bzw. Automatisierung, da sich moderne Industriegesellschaften in den letzten Jahrzehnten durch Technologisierung und Automatisierung sowie durch deren Verstetigung im Alltag der Menschen signifikant und nachhaltig verändert haben. Und die Verantwortlichen der Polizei mussten und müssen darauf reagieren; neben der mittlerweile üblichen Smartphone-Nutzung wird zukünftig vor allem eine funktions- und leistungsfähige Infrastruktur wesentlich werden. 2023 hieß es beispielsweise:

> „Bis 2030 soll die Polizei eine neue IT-Infrastruktur erhalten. Dafür schaffen die Innenministerien von Bund und Ländern derzeit die Voraussetzungen. (…) Im Kern drehen sich die Diskussionen um die Modernisierung der Polizeiarbeit darum, wie die deutschen Polizeien dem rasanten technologischen Fortschritt und den fortlaufenden gesellschaftlichen Veränderungen gerecht werden sollen“ (Fertig, 2023).

Die Polizeitechnik in Deutschland wird 2026 quasi 150 Jahre alt, denn bereits deutlich vor Ende des 19. Jahrhunderts verwendete die deutsche Polizei technische Hilfsmittel. „Von etwa 1876 an wurde mit dem Aufbau von Verbrecheralben begonnen, 1896 wurden die ersten Spurensicherungsdienste errichtet. Es bildeten sich, begünstigt durch die Anforderungen der Justiz nach gerichtsverwertbarer Beweisführung, der Erkennungsdienst und die naturwissenschaftliche Kriminaltechnik heraus“ (Heinrich, 2008, S. 290). Quasi im „Jubiläumsjahr“ 2026 erfolgt in diesem polizeihistorischen Beitrag eine jeweilige exemplarische Retrospektive auf einzelne Anwendungen von polizeilichen Ausrüstungsgegenständen, von technischen bzw. EDV-basierten Ermittlungshilfen oder auch von Maßnahmen für Ermittlungen und zur Gefahrenabwehr, die mit derartigen Mitteln und Methoden realisiert werden konnten.

Neben einer exemplarischen Nennung von Fiktionalem für die jeweilige Epoche, d. h., wie im Fernsehen oder Kino die ideale (im Sinne von erfolgreicher) Polizeiarbeit mit oder ohne Polizeitechnik dargestellt wurde, um auch den jeweiligen Zeitgeist kurz zu projizieren, erfolgt die kurze, kritische Reflexion, welche Risiken oder Gefahren dadurch direkt oder dabei indirekt innerhalb der Polizei bzw. für die Gesellschaft entstanden sind. (Staats-)kritisch kann man beispielsweise im Sommer 2026 fragen, ob die aktuelle Technik- und Schutzausrüstung der heutigen Polizisten im Streifendienst in der Summe nicht mehr die Uniform einer Bürgerpolizei ist, sondern diese vor allem dazu dient, die Polizei vor der Gesellschaft zu schützen, und sich die Polizisten dadurch bewusst von der Bevölkerung distanzieren oder sogar abgrenzen, da der Gesellschaft grundsätzlich eine Gewaltaffinität gegenüber der Polizei, ergo dem Staat, unterstellt wird.

Forschungsfrage und Methodik

Dieser Beitrag ist zweigeteilt: Neben dem deskriptiven Teil zur Polizeitechnikentwicklung wird jeweils untersucht, wie sich der Mensch (die Polizistin und der Polizist) durch den Technikeinsatz im Polizeidienst verändern kann bzw. konnte. Wenn man beispielsweise im Jahr 2026 durch den seit rund eineinhalb Jahrzehnten genutzten Digitalfunk über die Funkleitzentrale keine „persönliche“ Beziehung mehr zum anderen Menschen in Uniform hat bzw. signifikant weniger, dann kann dies auch das soziale Gefüge in einem Polizeipräsidium, die Kooperationsbereitschaft gegenüber der Funkleitzentrale oder das Vertrauen in die Kolleginnen und Kollegen beeinträchtigen. Die Kolleginnen und Kollegen der eigenen Dienstgruppe, aus der zuvor immer die Einsatzaufträge (bisweilen auch mit besonderen Hinweisen zur Orts- und/oder Personen-kenntnis) per Funk übermittelt wurden, kennen sich in der Regel untereinander und wissen um die Stärken und Schwächen der Dienstgruppenmitglieder, die für einen bestimmten polizeilichen Einsatz von Vor- oder Nachteil sein können, sei es die häusliche Ge-

walt, die Nachbarschaftsstreitigkeit, der Einsatz im Jugendhaus oder der Lkw-Unfall. Bei der bloßen Zuteilung der Funkleitzentrale einer „freien“ Streife für den nächsten abzuarbeitenden Einsatz bzw. derjenigen Streife, die am nächsten zum Einsatzort ist, ist dies nicht der Fall.

Die Forschungsfrage lautet, wie die Polizeitechnik den Menschen (die Polizistin und den Polizisten) verändert. Untersucht wird dabei, ob die Polizeitechnik Polizisten zu bloßen Ausführenden bzw. Anwendern (zum Technikbeiwerk) macht oder deren Kompetenzen und Fertigkeiten adäquat optimiert. Eine Teilfrage lautet, wie am Beginn dieses Beitrags bereits angedeutet, ob und wie die Polizei auf gesellschaftliche, soziale oder politische Veränderungen reagierte.

Die methodische Vorgehensweise basiert 1. auf einer (historischen) Quellenanalyse und 2. auf einer Beobachtung (die grundsätzlich nie wertfrei ist). (Polizei-)Historische und gesellschaftliche sowie aktuelle Entwicklungen werden dafür jeweils kurz dargestellt. Die Spezifika, wer alles Polizei ist – die Bundespolizei (die seit der Reformierung des Bundesgrenzschutzes nach der Jahrtausendwende mittlerweile automatisiert komplexe grenz- und bahnpolizeiliche Aufgaben mit perfektionierter Polizeitechnik wahrnimmt), das Bundeskriminalamt (der von Horst Herold veranlasste Reformprozess Anfang der 1970er Jahre gilt als Hauptinitiative für die Modernisierung der damaligen Kriminal- bzw. Polizeitechnik), die jeweilige Länderpolizei (mit technisch unterschiedlichen Standards bei deren Landespolizei, Bereitschaftspolizei, Landeskriminalamt oder Polizeihochschulen) oder die Polizei beim Deutschen Bundestag und die kommunale Vollzugspolizei –, ist in ihrer Diversität für diesen Beitrag ebenso wenig relevant wie die Unterscheidung von Polizeitechnik in Funktionsklassen (wie etwa in Kriminaltechnik, Informations- und Kommunikationstechnik, Überwachungstechnik oder Polizeitechnik in Form der Handschließe o. ä.). Exemplarisch verwies Heinrich (2008, S. 290) auf Folgendes: „Denkbar ist z. B. die Systematisierung nach Technikgattungen (…), nach dem Verhältnis zwischen Polizei und Techniknutzung bzw. Technikeinführung (…) oder nach Funktionsklassen (…).“ Im neuen Jahrtausend begann auch die systematische „Typologisierung der Einsatztechniken (…) in verschiedenen Ansätzen“ (ebd.), wobei die Relationen zur Kriminalpolitik oder einzelnen Politikfeldern hergestellt wurden, was im Kontext der Verwissenschaftlichung der Polizei realisiert wurde – nicht nur, um neue Erkenntnisse für die Polizeiwissenschaft zu erhalten, sondern auch, um die polizeiliche Arbeit mit entsprechender Polizeitechnik zu optimieren.

Operationalisierung und Epochenkreierung

Mit Automatisierung ist in diesem Beitrag das Bestreben der Polizei definiert, durch den systematischen Einsatz von Polizeitechnik polizeiliche Aufgaben und Verantwortlichkeiten (für Sicherheit und Ordnung zu sorgen, Kriminalität zu bekämpfen, präventiv und bürgernah tätig zu sein usw.) wahrzunehmen oder innezuhaben. Zur Klassifikation, wie sich die Polizeitechnik entwickelte, sind für diesen Beitrag selbstständig drei Epochen der Polizeitechnik kreiert und in den folgenden Hauptkapiteln skizziert: 1. Die 1970er und 1980er Jahre, 2. die 1990er und 2000er Jahre und 3. die 2010er und 2020er Jahre. Im letzten Kapitel erfolgt eine Kurzbewertung über die machbare bzw. realistische Polizeitechnik der Zukunft ab 2030. Da in diesem Sammelband zahlreiche aktuelle Beispiele von Polizeitechnik (wie

die mobilen Technologien, diverse Informationssysteme, Datenarchitekturen oder einzelne KI-Anwendungen) dargestellt sind und die 2020er Jahre noch andauern, ist das Kapitel über die 2010er und 2020er Jahre entsprechend kurz.

Die 1970er Jahre waren wie die 1980er Jahre von der Erkenntnis geprägt, dass der wirtschaftliche und technologische Fortschritt an seine Grenzen kommen kann und vor allem auch Gefahren, Risiken und Schaden verursacht – „(…) die Umweltverschmutzung durch die gestiegene Mobilität, großflächige Schäden durch freigesetzte toxische Industriestoffe, Unglücke aufgrund nicht eingehaltener Sicherheitsvorschriften (…) oder technische Katastrophen wie Flugzeugabstürze oder der Unfall im Kernkraftwerk Three Mile Island/Pennsylvania/USA“ (Beier, 2025, S. 24) sind Beispiele dafür. Der stetig wachsende Wohlstand fand auch in der gestiegenen Arbeitslosigkeit eine weitere Restriktion. Auch wenn Technik zu Negativem führen konnte, den Alltag bestimmte diese noch nicht.

In Privathaushalten hatte der tragbare CD-Player zum Ende der 1980er Jahre den Walkman ersetzt, und der offiziell von 1983 bis 1991 in Deutschland etwa 250.000 Mal verkaufte Commodore Personal Computer 64, weltweit waren es ca. 17 Millionen Stück (siehe dazu u. a. Steil, 2011), wurde in der nächsten Epoche durch diverse Spielekonsolen ausgetauscht – wesentlich mehr Technik gab es im Grunde nicht, denn beispielsweise Airbag, Zentralverriegelung oder elektrische Fensterheber wurden erst in den 1990er Jahren zur Sonderausstattung und dann zur Standardausrüstung in Kraftfahrzeugen.

Eine Ambivalenz prägte die 1990er und 2000er Jahre, nicht nur durch eine dynamisierte Atomisierung und Fragmentierung in der Gesellschaft bzw. in den Gesellschaftsschichten (sei es 1. in der Berufswelt, 2. durch den Bolognaprozess im akademischen Bereich oder 3. bei der Realisierung neuer Lebensmodelle, Begriffe wie Freizeitgesellschaft oder gleichgeschlechtliche Partnerschaften wurden zu Beginn des neuen Jahrtausends Normalität), sondern auch einerseits durch das Ende des Kalten Krieges – was die Internationalisierung und die Globalisierung erst ermöglichte und sich durch das seit Mitte der 1990er Jahre genutzte Internet dynamisierte (die Welt wurde dadurch kleiner, da man, wenn auch nur virtuell, näher und häufiger „zusammenkam“), Freiheit, unendliche Möglichkeiten und Zuversicht können dafür als Synonyme verwendet werden –, und andererseits exemplarisch 1. durch den Zerfall Jugoslawiens und die daraus resultierenden zermürbenden Kriege bis 2001 sowie 2. durch die Anschläge vom 11. September 2001 und die folgenden Jahre der schrecklichen und lang anhaltenden Angriffskriege der USA in Afghanistan und dem Irak oder 3. durch das Platzen der Dotcom-Blase im März 2000 – Angst, Misstrauen und Unsicherheit wären Begriffe dafür.

Die Videokassetten verschwanden sukzessive, die DVDs ersetzten diese. Digitalkameras wurden ab Mitte der 1990er Jahre auch im journalistischen Bereich verwendet, ein Jahrzehnt später auch in Privathaushalten, die Mikrowelle wurde zur Standardausstattung in der Küche, im Sport etablierten sich einfache Brustgurte mit Pulsuhren, das TV-Angebot stieg exponentiell – Automatisierung und Technik hatten noch keine Deutungshoheit, sie wurden aber in allen gesellschaftlichen Bereichen deutlich (sichtbar).

Die 2010er und 2020er Jahre brachten keine Beruhigung, neben den ebenso exemplarisch negativen Folgen des Arabischen Frühlings folgte eine Krise der nächsten: Die Finanzkrise der Jahre 2007 und 2008 mutierte zur Griechenland-, Euroschulden- und Staatsschulden-

krise, die weltweiten (Staats-)Schulden vervielfachten sich in den letzten 15 Jahren auf mittlerweile ca. 340 Billionen US-Dollar (Institute of International Finance, 2025), es folgten der Brexit von 2016 bis 2020, die Migrationskrise(n) seit 2015, die Coronarestriktionen von 2020 bis 2022 mit deren wirtschaftlichen und sozialen Spätfolgen sowie die Kriege in der Ukraine, im Gazastreifen oder im Iran. 2026 befindet man sich mitten in unsicheren Zeiten, Zukunftsängste, Sorgen und Wohlstandsverlust werden immer relevanter für die Menschen in der Bundesrepublik Deutschland und auch in anderen Regionen weltweit.

Der Mensch kommt zudem oftmals nicht mehr zur Ruhe: Sowohl Fitnesstracker als auch Smartphones sind täglich 24 Stunden und sieben Tage die Woche im Einsatz bzw. verfügbar (auch im Schlaf), der Thermomix ermöglicht auch dem Ungeübten das Kochen hochwertiger Gerichte (ein gewisser Perfektionierungszwang ist allgegenwärtig), Kraftfahrzeuge sind 2026 verpflichtend mit Geschwindigkeitsüberschreitungswarnton, mit Black Box oder Geschwindigkeitsassistenten ausgerüstet, Service- bzw. Software-Updates im Kraftfahrzeug erfolgen automatisiert über das Internet. Automatisierung und Technik, die Kundendatenauswertung beim bargeldlosen Bezahlen, das tägliche milliardenfache Datenüberwachen bzw. -abgreifen oder die absolute Vernetzung eines Haushaltes mit dem Internet (per Router, Solaranlage, Überwachungskamera, Stromzähler oder TV-Gerät) haben die Freiheit und die Individualität des Menschen marginalisiert, die Technik dominiert offensichtlich das Geschehen, den Alltag und oft auch den Menschen.

Die 1970er und 1980er Jahre: Rasterfahndung aus der Defensive

US-amerikanische Polizeiserien wie Starsky & Hutch oder Kojak stellten in den 1970er Jahren (Kriminal-)Polizisten oft mit Körpereinsatz dar, rennend, kletternd, springend oder prügelnd. In Deutschland hingegen galt das kriminalistische Gespür in Form der ruhigen, umsichtig agierenden, sachlichen Ermittler: Die Tatortkommissare (seit 1970 auf Sendung) oder Derrick (von 1974 bis 1998 auf Sendung) und „Der Alte“ (seit 1977 auf Sendung) sind dabei zu nennen. Die Polizei bzw. die ermittelnden Polizistinnen und Polizisten benötigten keine Polizeitechnik, vielmehr galt es, die möglichen Tatverdächtigen durch gezielte Fragen, logisches Kombinieren oder taktische und rechtlich zulässige Tricks zu ermitteln.

Polizeitechnik bestand damals vor allem aus dem „Fernmeldewesen“, dem „Kraftfahrzeugwesen“, aus „Hilfsmittel<n> der körperlichen Gewalt, Waffen und Gerät“ oder aus Spezifika für einzelne Polizeieinheiten wie etwa „Wasserfahrzeuge“, „Luftfahrzeuge“, „Technisches Gerät“ (wie dem „Absperrgerät“, dem „Sperrenbeseitigungsgerät“ oder dem „Beleuchtungsgerät“) oder „Verkehrsgeräte“ (wie dem „Gerät zur Verkehrsüberwachung“, dem „Gerät zur Unfallaufnahme“ oder dem „Gerät zur Verkehrserziehung“) sowie aus der „Datenverarbeitung“ (wie den „Datenverarbeitungsmaschinen und -anlagen“, dem „Datenträger“ oder der „Hardware“) und „Sicherungstechnik“, womit „Sicherheitskontrollen auf Flughäfen oder ähnlichen Anlagen“ gemeint waren (siehe die Kapitelüberschriften bei Uebe, 1982, S. 5–12). In den 1970er Jahren wurde die Polizeitechnik bei der Flughafensicherung zu einem wesentlichen Element der Inneren Sicherheit, denn die Innere Sicherheit wurde auch durch Entwicklungen im Ausland beeinträchtigt. BGS-Beamte unterwiesen in diesem Kontext beispielsweise peruanische Sicherheitskräfte mit Hand-Metalldetektoren (siehe dazu Bennewitz & Müller, 2022).

„Die Verflochtenheit von Innerer Sicherheit und internationalen Konflikten wurde bereits wenige Wochen nach dem Olympia-Attentat erneut deutlich, als Kommandos der ‚Popular Front for the Liberation of Palestine' (PFLP) die Lufthansa-Maschine ‚Kiel' entführten, um die drei überlebenden Attentäter des ‚Schwarzen Septembers' aus westdeutschen Gefängnissen freizupressen. (…) Die Lufthansa (…) sei durch die geplanten Prozesse gegen die Führungsriege der RAF besonders gefährdet, was den weltweiten Einsatz des BGS notwendig mache." (Bennewitz & Müller, 2022, S. 471−473).

Semerak (1988) unterteilte Polizeitechnik in „Fernmeldemittel", „Waffen", „Einsatzmittel", „Hilfsmittel körperlicher Gewalt", „Identifizierungsmittel" und „Datenverarbeitung (EDV)". Wie abstrakt und auch technokratisch damals Polizeitechnik war bzw. beschrieben wurde, verdeutlicht seine nachfolgende Beschreibung:

„Den Sammelbegriff für bewegliche und stationäre Fernmeldemittel der Polizei, bei denen der Übertragungsweg durch hochfrequente elektromagnetische Wellen gebildet wird, nennt man *Polizeifunk*. Er dient als Sprechfunkverbindung dem Nachrichtenaustausch zwischen Einsatzstellen (bzw. Befehlsstellen) und den eingesetzten Beamten sowie zwischen den Beamten selber. Durch den Einsatz des Polizeifunkes (sic!) ist die polizeiliche Arbeit erleichtert und effektiviert worden." (S. 127, kursiv im Original).

Die Rasterfahndung in der Bundesrepublik Deutschland (Horst Herold hatte bereits Ende der 1960er Jahre Ideen und Konzepte dafür präsentiert gehabt) sollte die polizeilichen Möglichkeiten zur Datenverarbeitung bzw. zur Verarbeitung und Auswertung mit Computern optimieren, denn geprägt waren die Anfangsjahre der 1970er Jahre auch durch eine behördliche Unübersichtlichkeit wegen des bürokratischen polizeilichen Meldewesens mit der immensen Anzahl von Fernschreiben, Statistiken (zu Tatorten oder Verbrechenshäufigkeiten) und Verfahrensvorschriften (Formularen u. Ä.) oder Steckbriefen – und all dies in Papierform. Das bundeseinheitliche Informationssystem der Polizei (INPOL) wurde 1972 eingeführt und 1976 zur Terrorismusbekämpfung das Datensystem für Personen, Institutionen, Objekte und Sachen (PIOS), es wurden dafür Reisedaten bzw. Flugdaten, Grenzübertritte oder Autovermietungen systematisch erfasst und dokumentiert, die Polizei konnte dadurch nach bestimmten Angaben (wie dem Alter oder der Herkunft von Personen) recherchieren (vgl. dazu Gugerli, 2009, S. 52 ff.). Der zur Verfügung stehende Haushalt des Bundeskriminalamtes hatte sich vom Beginn der 1970er Jahre bis 1978 auf fast 300 Millionen Deutsche Mark vervielfacht, 1978 waren im BKA rund 3.500 Personen beschäftigt. Das BKA wurde durch Horst Herold zum Vorbild bei der Polizeitechnik, die erforderlichen Ressourcen wurden dabei vom Bund zur Verfügung gestellt, einzelne Bundesländer konnten dabei bei ihren Polizeien nicht den jeweiligen technischen Fortschritten folgen. Anders war es bei der Polizeiausrüstung. Wegen der Gewalteskalation der RAF und durch den Deutschen Herbst wurde eines deutlich: „Die Politik reagiert: Die Polizei wird verstärkt, großkalibrige Waffen werden angeschafft, die Schießausbildung reformiert, Einsatzanzüge, Schutzhelme, Schutzschilde und moderne Schlagstöcke eingeführt" (Kühner & Debschütz, o. J., S. 136).

Der Wandel der Polizeitechnik beim BKA sollte sich im Nachhinein als wegweisend erweisen, denn die RAF-Mitglieder bzw. wenige Medien, die deren Ideologien und Forderungen verbreitet hatten, setzten in den 1970er Jahren lange Zeit Narrative über einen autoritären Staat. Es wurden Unwahrheiten verbreitet, dass der Staat 1. Inhaftierte foltere, zwar nicht

körperlich, aber die zeitweilige Einzelhaft von RAF-Mitgliedern müsse als „sensorische Deprivation“ (Kraushaar, 2007) gewertet werden, oder 2. gar ermordet habe (die Selbstmorde der RAF-Mitglieder in Stammheim sind bis heute ein Streitpunkt in bestimmten linken Gesellschaftsschichten). Die Polizei war dadurch, wie die Justiz, in die Defensive geraten, aber Polizeitechnik ermöglichte eine adäquate (und demokratische) Gegenreaktion, denn zunächst wurden die Maßnahmen des BKA zum Sammeln, Speichern und Auswerten von Daten in großen Teilen der Gesellschaft sowie in den Parteien kritisch bewertet, was sich im Deutschen Herbst jedoch änderte. Der Staat in Form der Polizei, der Justiz oder der Politik agierte zunächst aus der Defensive (dies war einer der Gründe dafür, dass zum Ende der 1970er Jahre begonnen worden war, die polizeiliche Öffentlichkeitsarbeit zu professionalisieren), man hatte der RAF zunächst die Deutungshoheit in den Medien überlassen. Für die Rasterfahndung – quasi aus der Defensive – wurden methodisch mithilfe von Computerauswertungen aus Massendaten wie Mietzahlungen oder Flugdaten Verdächtige herausgefiltert: Am 9. Juni 1979 hatte dies zur Festnahme von Rolf Heißler in Frankfurt am Main geführt, der dabei schwer verletzt wurde. Die Rasterfahndung als optimales Beispiel für erfolgreiche Polizeitechnik wurde nicht aus der Not heraus, sondern aus einer defensiven Position zunächst uneingeschränkt eingesetzt. Dabei versinnbildlicht sie den Beginn der datenbasierten bzw. automatisierten Polizeiarbeit, die den (Kriminal-)Polizisten vom kriminalistischen Gespür bzw. von der intuitiven Ermittlungsarbeit zur datenbasierten, systemgestützten Ermittlung führte: Die bisherige Polizeitechnik in Form von Funkgerät und Telefon wurde mit dem Computer und aktiver Fahndungsrecherche aktiver nutzbar. Aber auch das grundsätzliche Sammeln von Daten auf elektronischen, fotografischen oder anderen Datenträgern erwies sich als modern und hilfreich, wie etwa, als das BKA Anfang März 1986 die Annahme der schwedischen Sicherheitsbehörden nach dem Mord am schwedischen Regierungschef Olaf Palme zur Tatmunition widerlegte: Es handelte sich nicht, wie irrtümlich in Schweden angenommen, um eine spezielle Produktion, sondern um ein Massenprodukt, das lediglich in Schweden nicht erhältlich war, beim BKA aber katalogisiert worden war.

In der Retrospektive wurde Polizeitechnik in den 1970er Jahren vor allem auch als erforderliches Instrument zur Polizeiführung, zur Informationsverarbeitung und -koordination benötigt bzw. als dafür erforderlich gewertet. Der ehemalige Senator für Inneres der Hansestadt Bremen, Albert Lohse, beschrieb ein Praxisbeispiel folgendermaßen:

„Ich erinnere mich noch vor kurzer Zeit in Hamburg im dortigen Lagezentrum an eine schwarze Wandtafel, auf der in Form eines Durchführungsplanes die jeweilige Kräftelage dargestellt war. Da sich das Bild im Laufe des Einsatzes dauernd änderte, hatte ein Beamter den Auftrag, jede Situation vor ihrer Löschung – es wurde zünftig mit Kreide gearbeitet – fotografisch festzuhalten. Die Fotografien gaben später den tatsächlichen Ablauf wieder. Eine einfache aber wirkungsvolle Methode - und dies im Zeitalter der ADV“ (Lohse, 1978, S. 38).

Lohse wies vor fast einem halben Jahrhundert auch auf zukünftige Gefahren von computergesteuerten Fehlentscheidungen hin, seine Befürchtung einer „dem Computer angepaßten Sprech-, Denk- und Verhaltensweise (sic!)“ (S. 46) hat sich zwar nicht bestätigt, jedoch die der „Fehler- und Fälschungsmöglichkeiten“ und die einer „absoluten Überwachungsmöglichkeit“ (S. 45). Der technische, korrekter wäre der epochale, Umbruch fand aber tatsächlich erst in der folgenden Epoche statt, denn Anfang der 1990er Jahre wurden noch Fernschreiber, sogenannte Telex-Geräte mit Lochstreifen, als maschinelles Speichermedium für Text-

nachrichten verwendet (ehemalige Telex-Modelle siehe bei Siemens, o. O.). Der Wechsel des Nachrichtenversandes über Computer begann Mitte der 1990er Jahre. Im gleichen Zeitraum wurden seit Ende der 1980er Jahre komplexere Telefonanlagen zu einer wesentlichen Polizeitechnik, „ISDN-fähige Kommunikationsanlagen" (Schlüter, 1987) waren erforderliche Neuerungen, galt es doch, das störanfällige Fernsprechsondernetz bzw. Polizeisondernetz adäquat zu ergänzen und später ganz zu ersetzen. „Das Fernsprechsondernetz der Polizei wird als ein Führungs- und Informationsnetz für die Aufrechterhaltung der Inneren Sicherheit der Bundesrepublik Deutschland mit besonderen Leistungsmerkmalen betrieben, die über die der öffentlichen Dienste der Deutschen Bundespost hinausgehen" (Polizei-Führungsakademie, 1985, S. 22), hieß es damals. Die rasche Kommunikation zwischen den einzelnen Polizeien der westdeutschen Bundesländer, dem Bundesgrenzschutz oder dem Bundeskriminalamt, d. h. die unverzügliche polizeiinterne Nachrichtenübermittlung, aber auch mit anderen Institutionen der Inneren Sicherheit sowie mit der Bevölkerung in Notlagen waren damals wesentliche Zukunftsaufgaben (siehe dazu Beckebanze, 2000; Bergmann, 2005; Hamburger, 2005). Organisatorische Fragen zur Polizeitechnik betrafen am Ende der 1980er Jahre beispielsweise, wie viel Personal und wie viel sonstige Ressourcen für die Wartung und den Betrieb von Telefonanlagen benötigt würde – und diese technischen Neuerungen konnten durchaus als problematisch gewertet werden (vgl. dazu Brandt, 1989), denn man war durchaus auch kritisch eingestellt gegenüber „neuer" Polizeitechnik, trotz der Fahndungserfolge durch die Rasterfahndung oder des INPOL und technischer Ausrüstung wie Metalldetektoren.

Der Hollywood-Film RoboCop von 1987 war eine satirische Dystopie und keine Darstellung eines irgendwann einmal möglichen Versuchs, eine perfektionierte Polizeitechnik in Form der Symbiose von Mensch und Maschine zu zeigen. Verändert hat sich der Polizist in dieser Epoche nicht, aber der Einsatz von neuer Polizeitechnik ermöglichte eine schnellere Fahndungs- und Ermittlungsarbeit, die Polizei wurde modernisiert und dies erfolgte automatisiert. Und die Gesellschaft akzeptierte im Grunde die modernen Maßnahmen der Polizei zur Verbrechensbekämpfung.

Die 1990er und 2000er Jahre: Sammelabfragen zur Verfahrensvereinfachung

In den Hollywoodfilmen Staatsfeind Nr. 1 aus dem Jahr 1998 und Minority Report von 2002 werden unterschiedliche Formen staatlicher Überwachung thematisiert: Während Staatsfeind Nr. 1 die zur damaligen Zeit technisch möglichen Überwachungsmaßnahmen mithilfe von Verkehrskameras oder Satellitenaufnahmen darstellt, zeigt Minority Report fiktionale, allgegenwärtige Überwachungsmöglichkeiten in einem zukünftigen Überwachungsstaat, bei denen beispielsweise ständig und flächendeckend Iris-Scans der Augen im öffentlichen Raum erfolgen. Die Polizei bzw. der Staat wurden als Bedrohung für die Freiheit angesehen, und in Minority Report verhindert gar der Einsatz von Präkognition in Kombination mit hoch technologisierter Polizei- bzw. Überwachungstechnik Straftaten, bevor diese begangen werden können – die vermeintlichen Täter werden verhaftet und ohne ordentlichen Gerichtsprozess eingesperrt. Interessanterweise wandelte sich das Bild der Polizei bzw. der Polizistinnen und Polizisten in der Bundesrepublik Deutschland in den 1990er Jahren signifikant durch das Fernsehen, die RTL-Fernsehserie „Die Wache" oder die ARD-Fernsehserie „Großstadtrevier" zeigten die Polizei als Bürgerpolizisten, die stets für alle Sorgen und Nöte der Bevölkerung zur Verfügung standen. Später versinnbildlichten „Toto & Harry" bei RTL, wie

obrigkeitsstaatliche Autorität langsam verschwand (im Gegenteil zu den Hollywoodfilmen), aber Polizeitechnik spielte in den einzelnen Folgen nie eine wesentliche Rolle, sondern immer der Mensch in Uniform, der hilft. In den USA gab es bereits das Polizeirevier Hill Street (gesendet von 1981 bis 1987) und später NYPD (gesendet von 1993 bis 2005), die neben dem Dienstalltag auch die privaten Sorgen und Probleme der Polizisten thematisierten sowie den realen Alltag im Polizeidienst mit körperlicher Gewaltanwendung oder einer vulgären Aussprache darstellten – und auch dabei war Polizeitechnik nie der wesentliche Inhalt.

Anfang der 1990er Jahre verfassten die Polizisten den Vorkommnis-Bericht (auch als Tagesmeldung bezeichnet) und die Sachverhalte, die polizeirelevant waren (Verkehrsunfälle, Strafanzeige usw.) noch auf Schreibmaschinen: Oft mit drei- oder vierfachem Durchschlagpapier für die Dienststellenleitung, die Kriminalpolizei und die Direktionsleitung. Zu der Zeit wurde aber auch das neue Rechenzentrum im BKA Wiesbaden in Betrieb genommen, seitdem galt: „die Digitaltechnik ermöglicht neue Methoden der Phantombild-Erstellung“ (Bundeskriminalamt, 2012, S. 86), ergo erfolgte sie nicht mehr per Handzeichnung. Außerdem führte die Polizeitechnik zur intensiven Vernetzung, denn das „Automatisierte Fingerabdruck-Identifizierungssystem (AFIS) ist bundesweit betriebsbereit. Es bietet den Polizeien des Bundes und der Länder neben Personenrecherchen nun auch die Möglichkeit, am Tatort gesicherte daktyloskopische Spuren zu recherchieren“ (ebd., S. 88). Bereits in den 1990er Jahren wurden testweise Laptops verwendet (vgl. dazu Gaschar, 1991, S. 24ff.), die ersten Modelle der Polizei waren unhandliche, in einem sperrigen, schweren Metallkoffer befestigte Geräte, an denen auch ein Drucker angebracht war. Der Verfasser testete eines dieser Geräte Mitte der 1990er Jahre mehrere Wochen im Streifendienst beim Polizeirevier Nürtingen (bei Esslingen, BW), der gesamte Aufbau wog über 12 kg, der Drucker oder der Laptop funktionierten oftmals nicht (nach der Testphase wurde das Projekt eingestellt).

Anfang des neuen Jahrtausends waren der „Genetische Fingerabdruck“, die „digitale Signatur in der Polizei“, „Ermittlungen im Internet“, der „Digitalfunk“ (vgl. dazu das Inhaltsverzeichnis bei Polizei-Führungsakademie, 2001, S. 3), „Technische Führungs- und Einsatzmittel für die Eigensicherung“, „Polizeiliche Anwendungsfelder der Foto- und Videotechnik“, „Technische Grundlagen und derzeitiger Stand der analogen und digitalen Fotografie“, die „Computergestützte Auswertung von Videosignalen für polizeiliche Zwecke“, „Technische Möglichkeiten der computergestützten Bild- bzw. Videoauswertung“ oder die „Verbesserung und Authentisierung digitaler Bilder“ (vgl. dazu das Inhaltsverzeichnis bei Polizei-Führungsakademie, 2002, S. 3) wesentliche Aspekte der modernisierten Polizeitechnik, wobei das exponentiell gewachsene Aufgabenspektrum der deutschen Polizei deutlich wurde. Die Vernetzung, der sekundenschnelle Datenaustausch oder die Übertragung und Auswertung von größeren Datenmengen in immer kürzerer Zeit wurden im dienstlichen Alltag wichtiger. Hinzu kam, dass durch standardisierte Zugriffe jedes einzelnen Polizeiangehörigen auf Datenbanken der Zeitaufwand reduziert werden konnte. Die wesentliche Zeitersparnis lag aber auch darin begründet, dass manuelle Prüfungen automatisiert werden konnten, wodurch sich der Fokus der polizeilichen Ermittlungsarbeit von der routinemäßigen und zeitaufwendigen Arbeit zur Analyse entwickelte bzw. verschob. Die Effizienz wurde signifikant erhöht, erste Gefahren einer Massenüberwachung wurden jedoch deutlich. Im POLAS wurden Massenabfragen zur Routine, Sammelabfragen ermöglichten Massenabfragen in Registern, Hotel-Meldebescheinigungen wurden im Nachtdienst per Excel-Tabelle übersandt und blockweise in das POLAS kopiert. Massen-DNA-Tests oder die Aufklärung von Jahrzehnten

zurückliegenden Kapitalverbrechen verdeutlichten die Möglichkeiten der neuen Polizeitechnik. Einerseits war diese für die Gesellschaft sichtbar, etwa in modernen Streifenfahrzeugen oder in der polizeilichen Ausrüstung, andererseits vollzog sie sich für die Bürgerinnen und Bürger nicht sichtbar: Mit der zur Verfügung stehenden Polizeitechnik wurde ermittelt, analysiert, überwacht, ausgewertet, bewertet oder geplant.

Für den Bundesgrenzschutz galt seit dessen Gründung die stete Erweiterung und Verbesserung der polizeitechnischen Ausrüstung als Dogma, im neuen Jahrtausend wurde dies besonders deutlich. Exemplarisch ist dabei für die seit dem 1. Juli 2005 als Bundespolizei bezeichnete Behörde der „Polizeihubschrauber vom Typ Puma“ zu nennen: „Wie wichtig ständiges Üben ist, zeigte sich auch im Sommer 2005. Innerhalb kürzester Zeit standen drei BGS-Hubschrauber bei der Bekämpfung der Waldbrände in Portugal bereit“ (Scholzen, 2006, S. 153). Nicht nur die Grenzschutztruppe 9, sondern auch andere Einheiten des BGS bzw. der Bundespolizei waren und sind polizeitechnisch auf einem hohen Niveau in Europa, ebenso wie zahlreiche Spezialeinheiten der Länderpolizeien.

Während die bürgerkriegsähnlichen Zustände mit jeweils Dutzenden, teilweise schwer verletzten Polizisten bei den gewalttätigen Demonstrationen in Gorleben, Wackersdorf, Brokdorf oder in der Hamburger Hafenstraße – das Negativereignis war die Ermordung der zwei Polizisten am 2. November 1987 an der Startbahn West des Frankfurter Flughafens – die vorherige Epoche geprägt hatten, wurde das öffentliche Bild der Polizei ab den 1990er Jahren ein anderes, auch ohne neue Polizeitechnik. Die Jugendsachbearbeiter lasen selbstverständlich die dienstlich abonnierte Jugendzeitschrift BRAVO, die Öffentlichkeitsarbeit wurde optimiert, auch mit einer proaktiven Einstellungswerbung bei verschiedenen Messen, polizeiliche Kontaktbeamte für Moscheen und ähnliche Funktionen wurden etabliert. Polizeitechnisches Gerät und Ausrüstungsgegenstände der Polizei als Symbol der Staatsmacht bei den jeweils mehrere Tage andauernden Castor-Transporten zwischen 2001 und 2011 wurden weniger als Bedrohung, sondern vielmehr als Notwendigkeit gewertet, die transparente polizeiliche Öffentlichkeitsarbeit bei diesen Einsätzen war ein positiver Faktor dafür. Die Polizeitechnik wurde Alltag im Polizeidienst, immer mehr und neuere Methoden und Ausrüstungsgegenstände kamen hinzu, die menschliche Komponente des Polizisten war bzw. blieb aber weiterhin wesentlich.

Künstliche Intelligenz war in der Polizeipraxis noch nicht relevant, im Bereich der Polizeiforschung wurde diese damals u. a. folgendermaßen definiert: „Die künstliche Intelligenz wird als ein Fachgebiet innerhalb der Informatik eingestuft, unterliegt jedoch vielfältigen Einflüssen aus anderen Gebieten, z. B. der Psychologie, der Physiologie, der Pädagogik, der Linguistik und anderen“ (Polizei-Führungsakademie, o. J., S. 102), wobei noch keine Systematik hinter der Verwendung des Begriffes erkennbar war und auch keine konkreten Anwendungsgebiete für die Polizei präzisiert werden konnten. Ganz anders ist dies heute.

Die 2010er und 2020er Jahre: Aufrüstung der Streifenfahrzeuge und der Polizistinnen und Polizisten

US-amerikanische Krimiserien wie CSI dominieren von der Anzahl und der Sendehäufigkeit im deutschen Fernsehen die Polizeiserien, bis ins kleinste Detail werden in diesen jegliche Spuren mit der modernsten Polizeitechnik gesucht, geprüft, analysiert und bewertet. Deutsche Krimiserien wie SOKO 5113 (von 1978 bis 2015 auf Sendung, der Nachfolger SOKO München wurde Ende 2020 eingestellt) oder SOKO Leipzig (seit 2001 auf Sendung) zeigen die kriminalpolizeiliche Arbeit, wobei die Zusammenarbeit der einzelnen SOKO-Mitglieder wesentlich ist (und auch deren Privatleben), die hochtechnologisierten ermittlungs- und Überwachungsmöglichkeiten der Polizei sind sekundär. Anders ist es im Science-Fiction-Film Mercy mit Chris Pratt von 2026, in dem der Protagonist (ein Polizist des LAPD) vor Gericht auf einem Stuhl gefesselt ist, und er gegenüber dem Gericht in Form einer KI seine Unschuld beweisen muss: Die KI bestimmt, der Mensch ist nur Beiwerk.

In den 1990er Jahren wurden sichergestellte Mobiltelefone bzw. EDV-Beweismittel in der Regel bei den jeweiligen LKA ausgewertet, heutzutage erfolgt dies dezentral bei den Dienststellen durch zahlreiche qualifizierte Sachbearbeitende und die zur Verfügung stehende Polizeitechnik, denn diese ist seit den 2010er Jahren auch dezentralisiert worden. Polizeitechnik kann heutzutage zudem weiter definiert werden, auch der „Showroom für die Einbruchberatung" (Münchner Blaulicht, 2015, S. 209) ist darunter zu subsumieren, denn die „Verhinderung von Straftaten ist die vornehmste polizeiliche Aufgabe" (ebd., S. 208), und dies gelingt am besten mit einer bürgernahen Polizei. Mobile Scanner für Ausweise oder Kennzeichen können Echtzeitdaten übertragen, Überwachungsdrohnen mit Livebildern optimieren (Groß-)Einsätze und sind erheblich kostengünstiger als der Hubschrauber, und schließlich ist der elektronische Versand der Strafanzeige an die Staatsanwaltschaft zeitgemäß. Die Automatisierung bzw. Technologisierung bei der Polizei ist jedoch noch nicht vollendet, in Baden-Württemberg wechselte man beispielsweise 2026 vom analogen Farbmarkierungstraining zu lasergestützten Schießtrainingssystemen, die ein realitätsnahes und gefahrloses Training ermöglichen.

„Hierbei werden Laser-Module an einer Waffe angebracht. Bei der Abgabe eines simulierten Laser-Schusses werden Lichtimpulse von den Sensoren einer Trainingsweste erkannt und als simulierte Treffer angezeigt. (…) Die neuen lasergestützten Schießtrainingssysteme sind auch außerhalb von Einsatztrainings- und Schießstätten flexibel einsetzbar. Mit ihnen können Polizeibeamte etwa an einsatzrelevanten Örtlichkeiten wie Bahnhöfen, Schulen oder Flughäfen noch effektiver und realitätsnäher trainieren." (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, 2026).

Der Einsatz von Polizeitechnik professionalisierte und beschleunigte in allen drei skizzierten Epochen die Arbeit und ggf. auch den Ermittlungserfolg, was bei Straftaten wesentlich ist. In allen drei Epochen war und ist zudem die Infrastruktur einer der bedeutendsten Faktoren. Die negativen gesellschaftlichen Entwicklungen begannen schließlich zusätzlich das Bild der Polizei zu verändern – galt zum Beginn des neuen Jahrtausends noch die Maxime: „Grundsätzlich sollte sich die persönliche Ausstattung der Polizeibeamtin/des Polizeibeamten (sic!) an einem Erscheinungsbild orientieren, das dem Anspruch der bürgernahen Polizei gerecht wird. Techniken zur Bewältigung von Sondersituationen gehören in die Hände von Spezialeinheiten" (Kreitzberg, 2001, S. 38), so erfordern Amoklagen, das erweiterte Aufgabenspekt-

rum der Polizei oder die stetig ansteigende Gewalt gegen die Polizei, dass diese mit schwerer LABEL-Ausrüstung oder Bodycam im Einsatz ist bzw. sein muss. Polizisten sind zwar noch kein „Technikbeiwerk", obwohl Algorithmen Entscheidungen vorbereiten und menschliches Urteil ergänzen oder ersetzen, aber das äußere Erscheinungsbild hat sich geändert. Die Polizei und der Mensch im Polizeidienst wurden aufgerüstet: Sichtbar, aber auch nicht sichtbar, wenn Speicher-, Überwachungs-, Auswerte- oder Analysetechnik verwendet werden.

Die Science-Fiction-Polizei der Zukunft: Künstliche Intelligenz und wann kommt der RoboCop?

Künstliche Intelligenz bei der Polizei analysiert nicht nur einfache oder komplexere Bilddaten, sie erkennt auch Kriminalitätsmuster und unterstützt Predictive Policing, neben der Automatisierung von Routineaufgaben prognostiziert sie Trends und verändert dadurch die Polizeiarbeit durch Mustererkennung in Big Data, wie etwa bei der Nutzung der umstrittenen Palantir-Software. „In Deutschland findet der Einsatz von KI partiell im Bereich der Strafverfolgung und der Gefahrenabwehr statt. Die meisten Anwendungen und Projekte laufen im Rahmen des Bundeskriminalamtes" (Bitkom, 2023, S. 8). Das Menschsein und typische Eigenschaften, die für den Polizeiberuf relevant sind, wie die Empathie oder auch nach mehreren Berufsjahren die Intuition, können dabei verloren gehen. Auch wenn RoboCop-Szenarien Fiction bleiben, so macht eine Automatisierung die Polizei zu Überwachenden, was einer Entmenschlichung gleichkommen kann. Bereits heute ist der Polizist der Polizeitechnikbediener, was weitere menschliche Eigenschaften wie jahrzehntelanges Fachwissen, taktisches Vorgehen oder berufsethische Grundsätze mindern kann, weshalb ein Ausgleich zwischen polizeilicher Arbeitsroutine oder dem polizeilichen Ermittlungserfolg und den beruflichen ethischen Grundsätzen essenziell ist. Anders als in den 1970er Jahren bei der Rasterfahndung steigt durch die Verwendung von KI die Anforderung an die Polizei, die demokratischen und rechtsstaatlichen Grundsätze nicht zu negieren, denn allein bei der Anwendung von KI sind Gefahren und Risiken immanent (vgl. Beier, 2026). Ein (Polizei-)Überwachungsstaat Deutschland ist nicht abwegig, wenn man beispielsweise die KI-basierte digitale Gesichtserkennung auf Bahnhöfen bewertet. Mit „ihr werden ausnahmslos von allen Menschen, die an einer Kamera mit entsprechender Erkennungssoftware vorbeilaufen, personenbezogene Daten aufgenommen und die Ausprägung sichtbarerer Merkmale in Form von geometrischer Anordnung und Textureigenschaften der Oberfläche im Bereich des frontalen Kopfes analysiert. Die gespeicherten Daten werden anschließend mit Täterdateien abgeglichen." (Möllers, 2025, S. 39).

Bei der Bodycam ist beispielsweise „nicht auszuschließen, dass im Einsatz kontrollierte Personen einer filmtechnischen Aufzeichnung vor Ort widersprechen, weil sie dafür keine Rechtsgrundlage sehen" (Ley, 2026, S. 14), was zur Eskalation führen kann. Allgemein gilt: „Die Zuständigkeitsgliederung und das bürgernahe Prinzip vom Schutzmann an der Ecke kommen angesichts der zunehmenden Verfügbarkeit und Nutzung digitaler Technologien unter Druck" (Zink & Zimmermann, 2023, S. 1402). Früher haben Staaten bzw. Regierungen auch schon Daten gesammelt, heute erfolgt dies jedoch mit KI, was die Transparenz erheblich erschwert. Die technische und automatisierte Überwachung (mit oder ohne KI) ist neben einer restriktiven Rechtsprechung die wesentliche Machtbasis von autoritären Systemen, China gilt dabei als negatives Musterbeispiel mit mehreren Hundert Millionen genutzten Kameras und einem Social Scoring System mit stetem KI-Einsatz. Die Bundesrepublik Deutsch-

land ist davon noch entfernt. Die Science-Fiction-Polizei ist, wie oben kurz exemplarisch dargestellt, aber bereits Realität. Denn wenn für die Krawalle in der Nacht auf den 1. Mai 2026 in Berlin galt, dass „technisch alles aufgefahren oder in Bereitschaft gehalten [wurde], was möglich ist: Drohnenabwehr, Hubschrauber für Übersichtsaufnahmen, Boote, Wasserwerfer im Hintergrund für den Notfall, Fahrradstaffeln, Spürhunde, Kommunikationsteams, Klettereinheiten für die Sicherung von Dächern“ (WELT, 2026), dann verdeutlicht dies eine (ehemalige) Bürgerpolizei, die sich an gesellschaftliche, soziale und politische Veränderungen angepasst hat: weiterhin für die Bürger ansprechbar zu sein, zu helfen und zu schützen, aber auch bei entsprechenden Erfordernissen alle möglichen Arten der Polizeitechnik (zu Lande, zu Wasser und in der Luft) einzusetzen.

Die Polizei wurde in der Bundesrepublik Deutschland zur Bürgerpolizei und sie ist es in vielen Bereichen noch. Die Ausbildung und das Studium für den Polizeiberuf orientieren sich intensiv 1. an den zahlreichen einzuhaltenden und zu schützenden rechtlichen Gesetzen, Normen und Vorschriften, 2. daran, die gesellschaftlichen, sozialen und politischen Entwicklungen verstehen zu können sowie psychologische oder ethische Kenntnisse für das polizeiliche Handeln und Einschreiten gegenüber anderen Menschen zu erhalten, und 3. am Verantwortungsbewusstsein eines Bürgers im Dienste des Staates, aber auch im Dienste für seine Bürger, um den Rechtsstaat, die Demokratie und die Menschenwürde zu schützen, wobei die Polizeitechnik bei allen drei genannten Kriterien helfen kann.

Die Funktion und der Wesensgehalt der Polizistinnen und Polizisten in der Demokratie der Bundesrepublik Deutschland haben sich polizeihistorisch geändert, schließlich ändert sich auch jede Gesellschaft, jede Nation und jeder Staat im Verlauf der Jahrzehnte. Je nach Diensttätigkeit, nach Einsatzgeschehen sowie nach den zur Verfügung stehenden Ressourcen der Polizeitechnik und der Anzahl der Polizeiangehörigen kann die Polizei der Zukunft mit KI die Kriminalitätsbekämpfung, die Begleitung von Großveranstaltungen oder die Verkehrsüberwachung effizient und rechtsstaatlich adäquat gewährleisten. Gleichzeitig basieren auch die Organisationsstrukturen der Polizeien und deren systematisierte Arbeits- und Ermittlungsweisen auf gesellschaftlichen, sozialen oder politischen Veränderungen. Beide Bereiche und Perspektiven haben Risiken, beide bieten aber auch positive Möglichkeiten: KI (bzw. der Polizist als Ausführender) könnte in akuten Situationen beispielsweise verschiedene Sprachen sprechen (lassen), um mit ausländischen Straftätern zu kommunizieren, Live-Bilder per Drohne können die fehlenden Ortskenntnisse der Einsatzkräfte ergänzen, Anweisungen per Funk im Ohrstecker ebenso; die Möglichkeiten sind immens.

Technikbeiwerk sind der Polizist und die Polizistin noch nicht, dies könnte sich ab 2030 ändern, wenn Quantencomputer es ermöglichen, Drohnenschwärme nach vorheriger menschlicher oder auch KI-basierter Programmierung selbstständig steuern zu lassen, damit diese eigenständig Überwachungsaufgaben durchführen, Daten auswerten und dynamisch weitere Aktionen planen und ausführen. Vom RoboCop ist man aber noch weit entfernt.

Referenzen

Beckebanze, H. (2000). Können die künftigen öffentlichen UMTS-Mobilfunknetze die taktisch-betrieblichen Anforderungen der BOS an ein digitales Funk-Kommunikationssystem erfüllen? In Kuratorium der Polizei-Führungsakademie (Hrsg.): *Aktuelle Problemstellungen im Bereich der Polizeitechnik*. Schriftenreihe der Polizei-Führungsakademie, Bd. 4/2000, S. 7–12.

Beier, A. (2025). Die lange Geschichte der Menschheit wird durch die kurze Geschichte der KI nicht enden. Sicherheitsgefahren durch den Einsatz von Künstlicher Intelligenz: Genese. In Deutsches Polizeiblatt für die Aus- und Fortbildung: *Polizei und „Künstliche Intelligenz“*. 44. Jg., 6/2025, S. 23–26.

Beier, A. (2026). Künstliche Intelligenz – omnipotente Gefahren bei deren Anwendung sind Realität. Teil 1: Eine Kategorisierung für Technik & Mensch sowie Gesellschaft, Unternehmen und Staat. In Polizei Info Report: Heft 2/2026, S. 18–22.

Bennewitz, F., & Müller, M.-M. (2022). *Innere Sicherheit transnational:* Bundesdeutsche Polizeihilfe für Lateinamerika in den 1970er- und 1980er-Jahren. *Zeithistorische Forschungen/ Studies in Contemporary History, 19(3),* S. 457–481, https://doi.org/10.14765/zzf.dok-2469

Bergmann, L. (2005). Informations- und Kommunikationstechnologie in der Deutschen Polizei – Arbeit des UA IuK. In Kuratorium der Polizei-Führungsakademie (Hrsg.): *Ausgewählte Themen aus dem Technikspektrum der BOS*. Sächsisches Druck- und Verlagshaus, S. 7–12.

Bitkom e. V. (Hrsg.) (2023). KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung. Online: https://www.bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf

Brandt, H. (1989). Technik als „Kulturschock“ im polizeilichen Alltag? In BKA-Vortragsreihe: *Technik im Dienste der Straftatenbekämpfung*, Bd. 35.

Bundeskriminalamt (Hrsg.) (2012*). 60 Jahre Bundeskriminalamt. Eine Zeitreise 1951-2011*. Wirtschaftsverlag NW.

Fertig, M. (2023). *Wie Technologie die Polizeiarbeit verändert*. POLIZEI PRAXIS, https://www.polizeipraxis.de/ausgaben/2023/detailansicht-2023/artikel/wie-technologie-die-polizeiarbeit-veraendern-wird.html

Gaschar, W. (1991). *Die Laptop-Welle rollt*. Chip, Ausg. 5/1991, S. 24–28.

Gugerli, D. (2009). *Suchmaschinen: Die Welt als Datenbank*. Suhrkamp-Verlag.

Hamburger, G. D. (2005). GSM-Mobilfunknetze bei Großanlagen – Notfallkonzept eines Netzbetreibers. In Kuratorium der Polizei-Führungsakademie (Hrsg.): *Ausgewählte Themen aus dem Technikspektrum der BOS*. Sächsisches Druck- und Verlagshaus, Dresden, S. 13–20.

Heinrich, S. (2008). Kriminalpolitik und Entwicklung der Einsatztechniken in der Polizei. In Lange, H.-J. (Hrsg.): *Kriminalpolitik*. VS Verlag für Sozialwissenschaften, S. 289–306. https://doi.org/10.1007/978-3-531-90894-6_17

Institute of International Finance (2025). *IIF Global Debt Monitor. A New Wave of Debt Accumulation Ahead – Could This Time Be Different?* 9. Dezember 2025, S. 1, https://www.iif.com/LinkClick.aspx?fileticket=XaPrtyfpqD8%3D&portalid=0

Kinast, J. (2019). Nach Testphase – NRW-Polizei wird mit Smartphones ausgerüstet. In WESTDEUTSCHE ZEITUNG, https://www.wz.de/politik/landespolitik/nach-testphase-nrw-polizei-wird-mit-smartphones-ausgeruestet_aid-45719877

Kraushaar, W. (2007). Die Mythen der RAF. In *Bundeszentrale für politische Bildung*, https://www.bpb.de/themen/linksextremismus/geschichte-der-raf/49223/die-mythen-der-raf/#node-content-title-2

Kreitzberg, R. (2001). Technische Führungs- und Einsatzmittel für die Eigensicherung. In Polizei-Führungsakademie (Hrsg.) (2002*)*: *Polizeitechnik im Wandel. Internationales Seminar vom 12. bis 14. November 2001*.

Kühner, M., & Debschütz, H. (o. J.). *Blaulicht im Kessel. Stuttgarter Polizeigeschichte(n)*. Südverlag.

Ley, T. (2023). Der Einsatz audiovisueller Aufzeichnungstechnik im Polizeialltag in Form von Körperkameras. In Polizei Info Report: Heft 3/2023, S. 13–15.

Lohse, A. (1978): Rechnerunterstützte Einsatzhilfen als polizeiliches Führungsmittel. In Polizei-Führungsakademie (Hrsg.): Rechnerunterstützte Einsatzleitsysteme der Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Arbeitstagung vom 29. November bis 1. Dezember 1978 bei der Polizei-Führungsakademie in Münster.

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg (2026). *Lasergestützte Schießtrainingssysteme für die Polizei Baden-Württemberg*, Pressemitteilung vom 16. April 2026, Stuttgart.

Möllers, Martin H. W. (2025): Richtet sich die Reform des Bundespolizeigesetzes gegen das Grundgesetz? Eine staatsrechtliche Analyse der Berichterstattung in DER SPIEGEL. In Möllers, M. W. & Ooyen, R. C. van (Hrsg.): *Bundespolizei 2. Aktuelle verfassungsrechtliche Bezüge und Kontroversen*. Verlag für Polizeiwissenschaft, Frankfurt.

Münchner Blaulicht – Polizeiverein für Prävention und Bürgerbegegnung e. V. (Hrsg.) (2015). Chronik der Münchner Polizei. Hirschkäfer Verlag.

Polizei-Führungsakademie. Forschungs- und Entwicklungsstelle für Polizeitechnik (FEStPt) (1985). *Grobstudie „Führungs- und Einsatzmittel zur Kommunikation bei der Polizei“*, o. O.

Polizei-Führungsakademie. Forschungs- und Entwicklungsstelle für Polizeitechnik (FEStPt) (o. J.). *Tendenzen der Informationsverarbeitung und ihre zukünftige Nutzung in der Polizei*. o. O. (1996 wurde es in den HfPolBW-Bibliotheksbestand aufgenommen).

Polizei-Führungsakademie (Hrsg.) (2001). *Polizeitechnik im Wandel*. Internationales Seminar vom 05. bis 08. Juni 2000. Münster.

Polizei-Führungsakademie (Hrsg.) (2002). *Polizeitechnik im Wandel*. Internationales Seminar vom 12. bis 14. November 2001. Münster.

Schlüter, H. (1987). *ISDN-fähige Kommunikationsanlagen*. Net-Buch Telekommunikation, R. v. Decker Verlag, Heidelberg.

Scholzen, R. (2006): *Der BGS. Geschichte der Bundespolizei*. Motorbuch Verlag, Stuttgart.

Semerak, A. F. (1988). *Die Polizei in der Bundesrepublik Deutschland. Geschichte. Organisation. Dienstzweige. Funktionen. Aufgaben und Befugnisse. Polizeitechnik*. R. v. Decker & C. F. Müller Verlagsgesellschaft, Heidelberg.

Siemens (o. J.). *Lochstreifen rationalisieren*. https://www.cryptomuseum.com/telex/siemens/files/Lochstreifen_rationalisieren.pdf

Steil, M. (2011). *How many Commodore 64 computers were really sold?* https://www.pagetable.com/?p=547

Uebe, W. (1982). T*aschenbuch der Polizeitechnik*. Unter Mitarbeit von Böker, F., Lück, S., & Schulze, E.-W. Richard Boorberg Verlag.

WELT (2026). *„An der Zeit, unsere Wut zu nutzen" – 2600 Menschen bei Demo in Berlin, vereinzelt Zwischenfälle*, https://www.welt.de/vermischtes/article69f3fd4c6fe2dee7bfb0f4de/walpurgisnacht-an-der-zeit-unsere-wut-zu-nutzen-2600-menschen-bei-demo-in-berlin-vereinzelt-zwischenfaelle.html

Zink, W., & Zimmermann, K. (2023): Öffentliche Akzeptanz der Digitalisierung bei der Polizei. In Wehe, D., & Siller, H. (Hrsg.): *Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis.* 2., vollständig u. überarb. Aufl. Springer Gabler, Wiesbaden, S. 1401−1409.

Von der Insellösung zur Datenplattform: Entwicklungslinien polizeilicher Datenarchitekturen seit 2000 und ihre organisatorischen Folgen

Anosch Amanat

Polizeiliche Arbeit ist seit jeher auf Informationen angewiesen. Verändert hat sich jedoch die technische und organisatorische Ordnung, in der diese Informationen erhoben, gespeichert, ausgetauscht und ausgewertet werden. Um die Jahrtausendwende war die polizeiliche Informationsverarbeitung in Deutschland noch stark durch fachlich spezialisierte und weitgehend voneinander getrennte IT-Verfahren geprägt. Diese Systeme waren auf konkrete Aufgaben und Zuständigkeiten zugeschnitten, erschwerten jedoch die organisations- und behördenübergreifende Nutzung vorhandener Informationen. Mit wachsenden Anforderungen an Vernetzung, Auswertung und Zusammenarbeit geriet diese Architektur zunehmend unter Veränderungsdruck. Polizeiliche IT sollte nicht länger nur einzelne Arbeitsabläufe digital unterstützen, sondern Informationen über Verfahrens- und Zuständigkeitsgrenzen hinweg verfügbar und nutzbar machen (Bundesministerium des Innern und für Heimat, 2023; Ratcliffe, 2016). Der Übergang von fachlich abgegrenzten Insellösungen über Integrationsansätze hin zu plattformorientierten Datenarchitekturen reicht über technische Modernisierung hinaus. Daten werden weniger eng an einzelne Anwendungen gebunden und können zunehmend für unterschiedliche operative, analytische und strategische Aufgaben erschlossen werden. Damit verändern sich auch die Bedingungen, unter denen Informationen sichtbar werden, Zusammenarbeit organisiert und polizeiliche Entscheidungen vorbereitet werden. Datenarchitekturen werden so zu einem Bestandteil der organisatorischen Infrastruktur polizeilicher Arbeit (Hohpe, 2024; Rashedi, 2022).

Der Beitrag untersucht diese Entwicklung aus einer organisationsbezogenen Perspektive. Im Mittelpunkt steht die Frage, welche organisatorischen Folgen mit dem Wandel polizeilicher Datenarchitekturen seit Beginn des 21. Jahrhunderts verbunden sind. Die zentrale These lautet, dass Datenarchitekturen polizeiliches Handeln strukturieren, ohne selbst formale Entscheidungsträger zu sein. Sie beeinflussen, welche Informationen verfügbar und miteinander verknüpfbar sind, welche Akteure auf bestimmte Informationsräume zugreifen können und welche Formen der Auswertung praktisch möglich werden. Damit ergänzen sie die technische und rechtliche Dimension polizeilicher Digitalisierung um eine organisationsbezogene: Architekturentscheidungen betreffen auch Informationsflüsse, Verantwortlichkeiten, Zusammenarbeit, Steuerung und die Entwicklung organisationaler Fähigkeiten (Münter, 2023; Orlikowski, 1992; Rashedi, 2022). Aus dieser Perspektive ist auch der polizeiliche Grundsatz „Taktik führt Technik“ (oder auch „Technik folgt Taktik“) neu zu betrachten. Er bleibt ein fachliches Korrektiv, muss in datenbasierten Arbeitsumgebungen jedoch um eine systematische Verzahnung von Fachlichkeit und Technik ergänzt werden.

Die Argumentation folgt dieser Entwicklung in vier Schritten. Zunächst werden die zentralen Begriffe und theoretischen Bezugspunkte geklärt. Anschließend wird die Entwicklung polizeilicher Datenarchitekturen seit etwa dem Jahr 2000 von fachlich abgegrenzten Insellösungen über Vernetzungs- und Integrationsbestrebungen bis zur Plattformorientierung nachgezeichnet. Darauf aufbauend wird untersucht, in welcher Weise Datenplattformen

als Organisationsfaktor wirken und insbesondere Informationsverfügbarkeit, Zusammenarbeit, Steuerung sowie organisationale Fähigkeiten verändern. Abschließend werden die daraus entstehenden Spannungsfelder und Gestaltungsfragen diskutiert und mit Blick auf die weitere Entwicklung datenbasierter und KI-gestützter Polizeiarbeit eingeordnet.

Theoretischer und begrifflicher Rahmen

Der Wandel von der Insellösung zur Datenplattform lässt sich nicht allein anhand technischer Merkmale erfassen. Begriffe wie Fachverfahren, Integration, Plattform, Ontologie oder Governance bezeichnen unterschiedliche Formen der Informationsverarbeitung, verweisen zugleich aber auf organisatorische Vorstellungen: darauf, wie Daten erhoben und genutzt, Zuständigkeiten abgegrenzt, Zugriffe geregelt und Entscheidungen vorbereitet werden. Die begriffliche Klärung dient deshalb nicht nur der technischen Unterscheidung verschiedener Architekturen. Sie schafft den Rahmen, um deren organisatorische Bedeutung zu analysieren und technische Modernisierung nicht vorschnell mit organisatorischem Fortschritt gleichzusetzen (Orlikowski, 1992; Star & Ruhleder, 1996).

Einen Ausgangspunkt bildet der Begriff der datengetriebenen Polizeiarbeit. Er bezeichnet hier eine Form polizeilicher Aufgabenwahrnehmung, in der vorhandene Informationen systematisch verfügbar gemacht, verknüpft, ausgewertet und in operative wie strategische Entscheidungsprozesse einbezogen werden. Damit ist keine automatisierte Ableitung polizeilicher Entscheidungen aus Daten gemeint. Polizeiliches Handeln bleibt rechtlich gebunden, fachlich zu verantworten und kontextabhängig zu bewerten. Datengetriebene Polizeiarbeit erweitert vielmehr die Informationsgrundlage, auf der Ermittlungen, Auswertungen, Lagebilder und Führungsentscheidungen beruhen und knüpft insofern an Ansätze informationsgeleiteter Polizeiarbeit an (Ratcliffe, 2016).

Unter einer Insellösung wird im Folgenden ein informationstechnisches System verstanden, das für einen begrenzten fachlichen Zweck entwickelt, einer bestimmten organisatorischen Zuständigkeit zugeordnet und nur eingeschränkt mit anderen Systemen verbunden ist. Solche Systeme entsprechen einer arbeitsteiligen Organisationslogik, in der unterschiedliche Aufgaben durch jeweils spezialisierte Verfahren unterstützt werden. Ihre begrenzte Anschlussfähigkeit wird dort zum Problem, wo polizeiliche Arbeit auf Informationen angewiesen ist, die über Verfahrens-, Dienststellen- oder Behördengrenzen hinweg verfügbar sein müssen. Die konkrete historische Entstehung solcher Strukturen und der daraus hervorgegangenen Legacy-Landschaften wird im folgenden Kapitel untersucht.

Datenintegration setzt an diesen Grenzen an. Sie bezeichnet die Verbindung bislang getrennter Systeme, Datenbestände oder Prozesse durch Schnittstellen, Austauschformate, Standards oder gemeinsame Datenmodelle. Der Begriff umfasst dabei mehr als technische Konnektivität. Daten können nur dann verlässlich in unterschiedlichen organisatorischen Kontexten genutzt werden, wenn auch Verantwortlichkeiten, Datenqualität, Berechtigungen und Nutzungsregeln aufeinander abgestimmt sind. Integration ist deshalb zugleich eine technische, semantische und organisatorische Koordinationsaufgabe (Calvanese et al., 2017; Gieß et al., 2023).

Eine Datenplattform geht über die fallweise Verbindung einzelner Fachverfahren hinaus. Sie bezeichnet eine Architektur, in der Daten stärker von einzelnen Anwendungen entkoppelt, nach gemeinsamen Regeln vorgehalten und für unterschiedliche Nutzungen bereitgestellt werden. Während in einer fachverfahrensorientierten Architektur die jeweilige Anwendung den Ausgangspunkt bildet und ihre eigenen Datenbestände erzeugt, rückt in der Plattformlogik der gemeinsame Datenraum stärker in den Mittelpunkt. Anwendungen greifen auf definierte Datenbestände, Schnittstellen und Berechtigungsstrukturen zurück, anstatt für jede neue Aufgabe erneut eine eigene Informationsbasis aufzubauen (Hohpe, 2024; Rashedi, 2022). Für die hier gewählte organisationsbezogene Perspektive ist anschlussfähig, dass die Plattformforschung digitale Plattformen nicht nur als technische Artefakte, sondern auch als soziotechnische Arrangements aus technischen Komponenten, organisatorischen Prozessen und Standards beschreibt (De Reuver et al., 2018). Plattformisierung ist dabei nicht mit bloßer Zentralisierung gleichzusetzen. Zentral gespeicherte Daten bilden noch keine Plattform im hier verwendeten Sinne. Kennzeichnend ist vielmehr, dass wiederkehrende technische Grundlagen so bereitgestellt werden, dass unterschiedliche fachliche Nutzungen auf ihnen aufbauen können. Eine Plattform fungiert damit als Ermöglichungsstruktur: Sie stellt gemeinsame Daten, Schnittstellen, Standards, Zugriffsmechanismen und technische Dienste bereit (Hohpe, 2024). Welche organisatorischen Möglichkeiten und Abhängigkeiten daraus entstehen, wird später gesondert untersucht.

Eine wesentliche Voraussetzung dafür ist semantische Anschlussfähigkeit. Technisch übertragbare Daten sind nicht automatisch fachlich vergleichbar oder miteinander verknüpfbar. Polizeiliche Informationen beziehen sich unter anderem auf Personen, Orte, Ereignisse, Objekte, Organisationen, Maßnahmen, Spuren und deren Beziehungen. Ein gemeinsames Daten- und Bedeutungsmodell beschreibt daher nicht nur Datenfelder, sondern auch die fachlichen Rollen und Beziehungen, in denen diese Entitäten auftreten können. Eine Person kann beispielsweise in unterschiedlichen Sachverhalten Beschuldigter, Zeuge oder Geschädigter sein. Dieselbe räumliche Entität kann je nach Kontext Tatort, Wohnort oder Kontrollort darstellen. Ontologien oder vergleichbare kontrollierte Begriffsmodelle machen solche Bedeutungen und Beziehungen explizit und schaffen damit eine gemeinsame semantische Grundlage für unterschiedliche Datenbestände. Interoperabilität setzt folglich neben technischen Schnittstellen auch gemeinsame oder zumindest übersetzbare Bedeutungsstrukturen voraus (Calvanese et al., 2017; Gieß et al., 2023).

Der Begriff der Datenarchitektur wird im Beitrag als übergeordnete Kategorie verwendet. Er bezeichnet die Ordnung, nach der Daten erhoben, gespeichert, beschrieben, verknüpft, zugänglich gemacht, geschützt und ausgewertet werden. Dazu gehören technische Komponenten wie Datenbanken, Schnittstellen, Metadatenmodelle und Zugriffssysteme ebenso wie organisatorische Regeln zu Zuständigkeiten, Rollen, Berechtigungen und Datenqualität. Datenarchitekturen sind deshalb nicht mit einer einzelnen Software gleichzusetzen. Sie bilden vielmehr die infrastrukturelle Ordnung, in der technische Systeme, organisatorische Prozesse und Formen der Datennutzung aufeinander bezogen werden (Marcucci et al., 2023; Star & Ruhleder, 1996).

Governance bezeichnet die verbindliche Steuerungsordnung dieser Infrastruktur. Sie umfasst Regeln, Rollen, Zuständigkeiten, Standards, Entscheidungswege und Kontrollmechanismen, die festlegen, wie Daten erhoben, gepflegt, verändert, verknüpft und für unter-

schiedliche Anwendungen genutzt werden dürfen. Governance betrifft damit nicht nur die Einführung einer Plattform, sondern ihren dauerhaften Betrieb und ihre Weiterentwicklung. Sie soll sicherstellen, dass technische Veränderung rechtlich zulässig, fachlich belastbar, organisatorisch verantwortet und langfristig beherrschbar bleibt (Marcucci et al., 2023).

Diese Begriffe erhalten ihre analytische Bedeutung vor dem Hintergrund organisations- und techniksoziologischer Überlegungen. Organisationen werden nicht ausschließlich durch formale Zuständigkeiten, Hierarchien und Rechtsnormen strukturiert. Auch Routinen, Informationsflüsse und technische Infrastrukturen prägen, welche Handlungsoptionen im Alltag praktisch verfügbar sind. Datenmodelle legen Kategorien fest, Berechtigungssysteme verteilen Zugänge, Suchfunktionen strukturieren Auffindbarkeit und Workflows geben bestimmte Bearbeitungswege vor. Solche technischen Strukturen determinieren polizeiliche Entscheidungen nicht, sie prägen jedoch die Bedingungen, unter denen Informationen wahrgenommen, verarbeitet und in Handlungen übersetzt werden können. Technik und Organisation stehen insofern in einem wechselseitigen Verhältnis: Organisatorische und fachliche Annahmen werden in digitale Systeme eingeschrieben, während diese Systeme ihrerseits auf Arbeitsweisen und Entscheidungsprozesse zurückwirken (Orlikowski, 1992; Star & Ruhleder, 1996).

Vor diesem Hintergrund ist auch der polizeiliche Grundsatz „Taktik führt Technik“ einzuordnen. Er bleibt ein wichtiges fachliches Korrektiv. Technische Lösungen müssen sich an polizeilichen Aufgaben, rechtlichen Befugnissen und taktischen Anforderungen orientieren. Technische Möglichkeiten können für sich genommen keine polizeiliche Praxis legitimieren. Als lineares Verhältnis greift der Grundsatz in datenbasierten Arbeitsumgebungen jedoch zu kurz. Sobald Datenmodelle, Suchlogiken, Berechtigungen oder Plattformarchitekturen festlegen, welche Informationen verfügbar und welche Zusammenhänge technisch darstellbar sind, gestalten sie zugleich Voraussetzungen fachlichen Handelns. Fachlichkeit definiert damit nicht lediglich Anforderungen, die anschließend technisch umgesetzt werden. Sie muss bereits an der Gestaltung der technischen Strukturen beteiligt sein, in denen spätere fachliche Entscheidungen vorbereitet werden. „Taktik führt Technik“ bleibt richtig, wenn damit die fachliche Zielsetzung gemeint ist. In datenbasierten Arbeitsumgebungen muss technische Gestaltung jedoch von Beginn an gemeinsam mit der Fachlichkeit verzahnt werden.

Der Übergang von Insellösungen über Integration zu Plattformen wird im Folgenden entsprechend nicht als linearer Austausch älterer durch leistungsfähigere Technik verstanden. Analytisch interessiert vielmehr, wie sich die zugrunde liegende Informationsordnung verändert: von Datenbeständen, die eng an einzelne Verfahren und Zuständigkeiten gebunden sind, über deren schrittweise Vernetzung bis zu Architekturen, in denen gemeinsame Datenräume eine größere organisatorische Bedeutung gewinnen. Auf dieser begrifflichen Grundlage lässt sich nun untersuchen, wie sich dieser Wandel in der polizeilichen Informationsverarbeitung seit Beginn des 21. Jahrhunderts entwickelt hat.

Entwicklungslinien polizeilicher Datenarchitekturen seit 2000

Die Entwicklung polizeilicher Datenarchitekturen seit Beginn des 21. Jahrhunderts verlief weder linear noch als vollständige Ablösung älterer durch neue Systeme. Technische Modernisierung traf vielmehr auf föderale Zuständigkeiten, rechtliche Zweckbindungen und his-

torisch gewachsene Fachlogiken. Neue Verfahren wurden eingeführt, während bestehende Systeme weiterbetrieben, erweitert oder über Schnittstellen angebunden werden mussten. Der Wandel vollzog sich deshalb schrittweise und unter Bedingungen, die technische und organisatorische Entscheidungen eng miteinander verknüpften.

Für die folgende Rekonstruktion lassen sich idealtypisch drei Entwicklungsphasen unterscheiden. In einer ersten Phase dominierten fachlich spezialisierte Verfahren und weitgehend voneinander getrennte Datenbestände. Darauf folgten verstärkte Bemühungen um Vernetzung und Integration. Seitdem gewinnt schließlich eine Plattformlogik an Bedeutung, bei der nicht mehr allein einzelne Verfahren oder deren Schnittstellen, sondern gemeinsame Datenräume und übergreifende Architekturen in den Mittelpunkt rücken. Diese Phasen lösen einander nicht vollständig ab. Vielmehr bestehen Fachverfahren, Integrationslösungen und Plattformansätze bis heute nebeneinander. Die Dreiteilung beschreibt daher keine strikt chronologische Abfolge, sondern einen Wandel der jeweils prägenden Architekturprinzipien.

Fachverfahren, Insellösungen und Legacy-Strukturen

Um das Jahr 2000 war die polizeiliche Informationsverarbeitung in Deutschland stark durch spezialisierte Fachverfahren geprägt. Vorgangsbearbeitung, Fallbearbeitung, kriminalpolizeiliche Auswertung, Asservatenverwaltung oder Einsatzdokumentation wurden vielfach durch jeweils eigene Systeme unterstützt. Diese Struktur entsprach der arbeitsteiligen Organisation der Polizei und ihren rechtlich wie fachlich abgegrenzten Zuständigkeiten. Für einzelne Aufgabenbereiche war es naheliegend, technische Verfahren zu entwickeln, die deren spezifische Anforderungen möglichst genau abbildeten (Bundesministerium des Innern und für Heimat, 2023). Die daraus entstandene Vielfalt war deshalb zunächst kein bloßes Modernisierungsdefizit. Unterschiedliche Aufgaben führten zu unterschiedlichen Datenmodellen, Eingabemasken und Bearbeitungsroutinen. Informationen wurden in dem fachlichen Zusammenhang erfasst und gespeichert, in dem sie benötigt wurden. Gerade diese enge Passung an einzelne Aufgabenbereiche begrenzte jedoch die Nutzbarkeit der Daten außerhalb des jeweiligen Verfahrens.

Mit zunehmender organisationsübergreifender Zusammenarbeit wurden die Grenzen dieser Struktur deutlicher. Informationen konnten in einem System vorhanden sein, ohne für andere Dienststellen oder Verfahren unmittelbar auffindbar zu sein. Daten mussten mehrfach erfasst, manuell übertragen oder über zusätzliche Kommunikationswege weitergegeben werden. Neben zusätzlichem Arbeitsaufwand entstanden dadurch unterschiedliche Informationsstände und zeitliche Verzögerungen. Die technische Trennung der Systeme wirkte sich somit unmittelbar darauf aus, welche polizeilichen Erkenntnisse an welcher Stelle verfügbar waren (Hollywood et al., 2015).

Langfristig verstärkte sich diese Fragmentierung durch die Art, wie neue fachliche Anforderungen häufig technisch beantwortet wurden. Für ein konkretes Problem wurde ein zusätzliches spezialisiertes Verfahren entwickelt oder beschafft. Dieses konnte die jeweilige Aufgabe kurzfristig verbessern, erzeugte aber zugleich einen weiteren Datenbestand, zusätzliche Schnittstellen und neue Betriebsabhängigkeiten. Mit jeder solchen Erweiterung stieg der Aufwand, die entstandenen Systeme später miteinander zu verbinden, zu migrieren oder ab-

zulösen. Auf diese Weise bildeten sich Legacy-Strukturen, deren Komplexität nicht auf eine einzelne Fehlentscheidung zurückzuführen war, sondern auf die kumulative Wirkung vieler fachlich nachvollziehbarer Einzelentscheidungen. Vergleichbare Effekte gelten auch in anderen Bereichen der öffentlichen Verwaltung als wesentliches Hindernis digitaler Transformation (Irani et al., 2023).

Der föderale Aufbau der deutschen Polizei verstärkte diese Entwicklung. Bund und Länder verfügen über eigene Zuständigkeiten, Organisationsstrukturen und historisch gewachsene technische Lösungen. Entsprechend entwickelten sich unterschiedliche Systemlandschaften, Datenmodelle und Modernisierungspfade. Diese Vielfalt war Ausdruck legitimer organisatorischer Eigenständigkeit, erschwerte jedoch dort die Zusammenarbeit, wo Informationen länder- oder behördenübergreifend genutzt werden mussten (Bundesministerium des Innern und für Heimat, 2023).

Der Bedarf an einem solchen Informationsaustausch nahm zugleich zu. Kriminalitätsphänomene wie organisierte Kriminalität, politisch motivierte Kriminalität, Cybercrime oder das Agieren überregionaler Tätergruppen ließen sich immer weniger innerhalb einzelner organisatorischer oder räumlicher Zuständigkeiten betrachten. Ermittlungsrelevante Zusammenhänge ergaben sich häufig erst aus der Verbindung verschiedener Informationen über Personen, Orte, Zeitpunkte, Tatmuster oder Beziehungen. Damit trat ein struktureller Widerspruch deutlicher hervor: Die Informationsverarbeitung blieb fachlich und organisatorisch fragmentiert, während die polizeiliche Praxis zunehmend auf übergreifende Erkenntniszusammenhänge angewiesen war (Ratcliffe, 2016). Dieser Widerspruch bildete einen wesentlichen Ausgangspunkt für die folgenden Integrationsbestrebungen. Die Herausforderung bestand darin, Informationsbestände über bestehende Verfahrens- und Zuständigkeitsgrenzen hinweg nutzbar zu machen, ohne die rechtlichen und organisatorischen Bindungen ihrer Erhebung aufzulösen.

Vernetzung, Integration und semantische Grenzen

Seit den 2000er Jahren verlagerte sich der Modernisierungsschwerpunkt deshalb zunehmend von der Digitalisierung einzelner Aufgaben auf die Verbindung vorhandener Informationsräume. Bestehende Fachverfahren sollten zunächst nicht vollständig ersetzt, sondern technisch und organisatorisch stärker miteinander verbunden werden. Schnittstellen, Austauschformate, gemeinsame Abfragemöglichkeiten und zentrale Komponenten sollten ermöglichen, Informationen über bisherige Systemgrenzen hinweg zu nutzen. Auch der Maßstab für die Leistungsfähigkeit eines Fachverfahrens veränderte sich. Entscheidend war nicht mehr allein, ob es seinen unmittelbaren Aufgabenbereich zuverlässig unterstützte. Zunehmend gewann auch die Frage an Bedeutung, ob die dort gespeicherten Informationen für andere polizeiliche Zwecke auffindbar und nutzbar gemacht werden konnten. Der einzelne Vorgang oder Fall wurde damit stärker als Bestandteil eines größeren Informationszusammenhangs betrachtet, der für Auswertungen, Lagebilder oder behördenübergreifende Ermittlungen relevant sein konnte. Forschung zum polizeilichen Informationsaustausch weist zugleich darauf hin, dass die tatsächliche Verfügbarkeit solcher Informationen neben technischen Voraussetzungen auch von rechtlichen, organisatorischen und praktischen Austauschbedingungen abhängt (Phythian et al., 2024; Ratcliffe, 2016).

Ein unmittelbares Ziel der Integrationsbemühungen bestand darin, Medienbrüche und Mehrfacheingaben zu reduzieren. Unterschiede zwischen Systemen betrafen jedoch nicht nur deren technische Verbindung. Abweichende Datenfelder, Katalogwerte, Schreibweisen und Aktualisierungsstände erschwerten auch die gemeinsame Nutzung der Informationen. Fragen nach Datenqualität, Pflegeverantwortung und verbindlichen Standards gewannen deshalb an Bedeutung. Integration erforderte zunehmend eine Abstimmung darüber, nach welchen Regeln Informationen erhoben und weiterverarbeitet werden sollten.

Gerade hier traten die Grenzen rein technischer Vernetzung hervor. Schnittstellen können Daten zwischen Systemen übertragen, gleichen jedoch unterschiedliche fachliche Logiken nicht automatisch aus. Informationen werden in konkreten Verfahren für bestimmte Zwecke und unter bestimmten rechtlichen Bedingungen erhoben. Ihre Bedeutung lässt sich deshalb nicht ohne Weiteres auf andere Nutzungskontexte übertragen. Unterschiedliche Kategorien, Erhebungsanlässe, Berechtigungen, Löschfristen und Zuständigkeiten mussten bei jeder weitergehenden Integration berücksichtigt werden. Besonders sichtbar wurde diese Grenze auf der semantischen Ebene. Technisch identische oder ähnlich bezeichnete Datenfelder können in verschiedenen Verfahren unterschiedliche Bedeutungen besitzen. Damit bestätigte sich eine bereits im begrifflichen Rahmen herausgearbeitete Voraussetzung: Interoperabilität erfordert neben technischen Schnittstellen auch abgestimmte Bedeutungsstrukturen. Für die historische Entwicklung ist an dieser Stelle vor allem relevant, dass mit fortschreitender Integration die Harmonisierung von Datenmodellen und Begriffssystemen selbst zu einem Gegenstand der Modernisierung wurde (Calvanese et al., 2017; Gieß et al., 2023).

In dieser Phase entstanden verschiedene Ansätze zur Modernisierung und Harmonisierung der polizeilichen Informationsverarbeitung. Ziel war unter anderem, zentrale Informationssysteme weiterzuentwickeln, länderübergreifende Abfragen zu erleichtern und gemeinsame Standards zu etablieren. Dadurch konnten bestehende Informationsbestände besser zugänglich gemacht werden, ohne die vorhandenen Fachverfahren unmittelbar vollständig ersetzen zu müssen (Bundesministerium des Innern und für Heimat, 2023). Die Grenze dieses Entwicklungsstadiums lag in der fortbestehenden Bindung der Daten an ihre unterschiedlichen Ausgangssysteme. Der Informationsaustausch verbesserte sich, während die zugrunde liegende Systemlandschaft weitgehend erhalten blieb.

Bestehende Verfahren mussten weiterbetrieben und durch zusätzliche Schnittstellen miteinander verbunden werden. Alte und neue Komponenten überlagerten sich, wodurch die Systemlandschaft teilweise noch komplexer wurde. Ein vollständiger Neuaufbau war angesichts organisatorischer, rechtlicher und finanzieller Rahmenbedingungen kaum realistisch, eine fortgesetzte Erweiterung der Schnittstellenarchitektur stieß jedoch ebenfalls an Grenzen (Irani et al., 2023).

Die wachsende Schnittstellenkomplexität rückte die Grundordnung der Datenhaltung zunehmend in den Vordergrund. Wenn jede neue Nutzung zunächst zwischen bestehenden Anwendungen vermittelt werden musste, blieb die einzelne Fachanwendung der strukturelle Ausgangspunkt der Informationsverarbeitung. Die zunehmenden Integrationsanforderungen legten deshalb einen weitergehenden Ansatz nahe, Daten nicht nur zwischen

bestehenden Systemen auszutauschen, sondern sie stärker aus der Bindung an einzelne Anwendungen zu lösen und in gemeinsamen, kontrolliert nutzbaren Strukturen bereitzustellen. An dieser Stelle beginnt der Übergang von der Integrations- zur Plattformlogik.

Plattformisierung polizeilicher Datenverarbeitung

Mit dem Übergang zur Plattformorientierung verändert sich die Leitvorstellung polizeilicher Informationsverarbeitung erneut. Während Integrationsansätze vor allem darauf zielten, bestehende Fachverfahren miteinander zu verbinden, setzt die Plattformlogik eine Ebene tiefer an: Daten sollen stärker aus der Bindung an einzelne Anwendungen gelöst, nach gemeinsamen Regeln vorgehalten und für unterschiedliche Nutzungen bereitgestellt werden. Damit verschiebt sich der architektonische Bezugspunkt. Nicht mehr allein das einzelne Fachverfahren oder die Schnittstelle zwischen mehreren Verfahren steht im Mittelpunkt, sondern eine gemeinsame Datenbasis, auf die unterschiedliche Anwendungen zugreifen können.

Diese Entwicklung entspricht einem allgemeinen Trend der digitalen Transformation, Daten als eigenständige und wiederverwendbare Ressource zu behandeln (Hohpe, 2024; Rashedi, 2022). Für die polizeiliche Informationsverarbeitung ist diese Verschiebung besonders weitreichend. Daten entstehen weiterhin in konkreten fachlichen Zusammenhängen, sollen aber zunehmend über ihren ursprünglichen Anwendungskontext hinaus nutzbar werden. Damit wächst die Bedeutung gemeinsamer Standards, Datenmodelle, Zugriffsmechanismen und technischer Dienste, die eine solche Nutzung erst ermöglichen.

Plattformorientierte Architekturen reagieren zugleich auf ein Problem, das sich in der Phase der Fachverfahren und der anschließenden Integration zunehmend verschärft hatte. Neue fachliche Anforderungen sollten nicht mehr regelmäßig dazu führen, dass zusätzliche Anwendungen mit eigenen Datenbeständen und individuellen Schnittstellen entstehen. Stattdessen sollen neue fachliche Produkte auf gemeinsamen technischen und datenbezogenen Grundlagen aufsetzen. Plattformisierung bedeutet daher nicht das Ende spezialisierter Anwendungen. Sie verändert vielmehr deren architektonische Einbettung. Neue Anwendungen sollen vorhandene gemeinsame Ressourcen nutzen, anstatt erneut eigenständige Informationsräume zu schaffen (Hohpe, 2024; Irani et al., 2023).

Die Modernisierung erhält dadurch einen anderen Charakter. Während die Integrationsphase bestehende Systeme vor allem nachträglich miteinander verband, verlangt Plattformisierung stärker nach einer gemeinsamen Grundordnung der Datenhaltung und -nutzung. Diese Veränderung lässt sich jedoch nicht als vollständiger Übergang von einer alten zu einer neuen Architektur verstehen. Bestehende Fachverfahren, Schnittstellen und Legacy-Komponenten bleiben während des Umbaus bestehen und müssen mit neuen Plattformstrukturen verbunden, migriert oder schrittweise abgelöst werden. Plattformisierung entsteht daher innerhalb einer bereits gewachsenen IT-Landschaft und nicht an deren Stelle.

Welche organisatorischen Folgen mit dieser Architekturverschiebung verbunden sind, etwa für Informationszugänge, Datenqualität, Zusammenarbeit, Steuerung oder die Entwicklung neuer fachlicher Anwendungen, wird im folgenden Kapitel gesondert untersucht. Für die

historische Entwicklung ist zunächst entscheidend, dass sich der Modernisierungsanspruch von der Verbindung einzelner Systeme auf die Gestaltung einer gemeinsamen Informationsarchitektur erweitert hat.

P20 als Verdichtungspunkt föderaler Plattformisierung

Im deutschen Polizeikontext lässt sich das Programm Polizei 20/20, später häufig als P20 bezeichnet, als Verdichtungspunkt dieser Entwicklung verstehen. Es markiert nicht den Beginn der Modernisierung polizeilicher Informationsverarbeitung, sondern bündelt Probleme und Reformansätze, die sich über einen längeren Zeitraum herausgebildet hatten. Einen wesentlichen Ausgangspunkt bildete die Saarbrücker Agenda zur Informationsarchitektur der Polizei aus dem Jahr 2016. Bund und Länder verständigten sich damit auf eine strategische Weiterentwicklung der polizeilichen IT mit dem Ziel, Informationen besser verfügbar zu machen, Wirtschaftlichkeit zu erhöhen und Datenschutz stärker durch technische Gestaltung zu unterstützen (Bundesministerium des Innern und für Heimat, 2023; Innenministerkonferenz, 2016).

Charakteristisch für P20 ist, dass unterschiedliche Modernisierungsprobleme nicht länger isoliert behandelt werden. Heterogene Fachverfahren, voneinander abweichende Datenmodelle, Mehrfacheingaben, Schnittstellenprobleme und föderal gewachsene IT-Landschaften erscheinen als miteinander verbundene Bestandteile einer übergreifenden Architekturfrage. Der Modernisierungsanspruch erweitert sich dadurch auf gemeinsame Standards und Strukturen, die eine länder- und behördenübergreifende Nutzung polizeilicher Informationen ermöglichen sollen.

Der föderale Kontext macht die Komplexität dieses Übergangs besonders sichtbar. Die bestehende IT-Landschaft ist über Jahrzehnte gewachsen und kann während der Transformation nicht außer Betrieb gesetzt werden. Fachverfahren müssen weiter genutzt, angebunden, migriert oder schrittweise ersetzt werden. Gleichzeitig bestehen unterschiedliche Zuständigkeiten, rechtliche Anforderungen und organisatorische Prioritäten fort. Die Entwicklung einer gemeinsamen Informationsarchitektur vollzieht sich deshalb parallel zum laufenden polizeilichen Betrieb und ist auf längerfristige Migrations- und Abstimmungsprozesse angewiesen.

P20 steht insofern exemplarisch für den Übergang von einer Modernisierung einzelner Systeme zu einer übergreifenden Architekturperspektive. Das Programm zeigt zugleich, dass Plattformisierung in einer föderalen Organisation nicht als einmaliger technischer Umbau verstanden werden kann. Zielarchitekturen müssen bestehende Strukturen aufnehmen und zugleich für zukünftige fachliche und technische Veränderungen offen bleiben. Die damit verbundenen Zielkonflikte zwischen Harmonisierung, föderaler Eigenständigkeit, rechtlicher Kontrolle und Entwicklungsfähigkeit werden später als eigene Spannungsfelder aufgegriffen.

Zwischenfazit: struktureller Wandel statt bloßer Technikmodernisierung

Die Entwicklung seit Beginn des 21. Jahrhunderts lässt sich damit als Veränderung der dominierenden Architekturprinzipien polizeilicher Informationsverarbeitung beschreiben. Fachverfahren richteten Datenhaltung zunächst vor allem an einzelnen Aufgaben und Zu-

ständigkeiten aus. Integrationsansätze versuchten anschließend, die daraus entstandenen Informationsräume stärker miteinander zu verbinden. Mit der Plattformorientierung verlagert sich der Schwerpunkt schließlich auf gemeinsame Daten- und Infrastrukturgrundlagen, die von unterschiedlichen Anwendungen genutzt werden können.

Diese Entwicklung ist jedoch nicht abgeschlossen und folgt keiner einfachen Ablösungslogik. Fachverfahren, Schnittstellenarchitekturen und Plattformansätze bestehen gleichzeitig fort und müssen miteinander verbunden werden. Gerade diese Überlagerung kennzeichnet den gegenwärtigen Zustand polizeilicher Informationsarchitekturen.

Der Wandel von der Insellösung zur Datenplattform bezeichnet deshalb weniger einen abgeschlossenen technischen Modernisierungspfad als eine Veränderung der strukturellen Ordnung polizeilicher Informationsverarbeitung. Welche Folgen daraus für Informationsflüsse, Zusammenarbeit, Steuerung und fachliche Handlungsmöglichkeiten entstehen, ist Gegenstand des folgenden Kapitels.

Datenplattformen als Organisationsfaktor

Die bisher beschriebene Verschiebung von fachlich getrennten Systemen zu gemeinsamen Datenarchitekturen verändert nicht nur die technische Verarbeitung polizeilicher Informationen. Sie wirkt auf Arbeitsabläufe, Informationszugänge, Zusammenarbeit und Steuerung zurück. Datenplattformen werden damit zu einem Organisationsfaktor: Sie treffen selbst keine polizeilichen Entscheidungen und verfügen über keine eigene rechtliche Zuständigkeit, gestalten aber die Bedingungen mit, unter denen Informationen verfügbar werden und Entscheidungen vorbereitet werden können (Orlikowski, 1992; Star & Ruhleder, 1996).

Diese Wirkung beginnt bereits mit der Reichweite polizeilicher Informationen. Daten entstehen weiterhin in konkreten Situationen, etwa bei Anzeigenaufnahmen, Vernehmungen, Kontrollen, Spurensicherungen oder Auswertungen. In einer fachverfahrensorientierten Architektur blieb ihre weitere Nutzung jedoch häufig an das jeweilige Verfahren und dessen organisatorischen Kontext gebunden. Plattformorientierte Architekturen können diese Bindung lockern: Informationen werden für weitere berechtigte Nutzer auffindbar, lassen sich mit anderen Beständen in Beziehung setzen und können in neue Auswertungszusammenhänge einfließen. Aus einer zunächst fall- oder vorgangsbezogenen Information kann damit eine organisationsübergreifend relevante Informationsressource werden.

Sichtbarkeit und polizeiliche Aufmerksamkeit

Sichtbarkeit ist eine zentrale Voraussetzung dafür, dass Informationen innerhalb der Organisation praktisch relevant werden können. Entscheidend ist, ob sie auffindbar, zugänglich und in einem auswertbaren Zusammenhang dargestellt sind. Informationen, die in isolierten Systemen verbleiben, können außerhalb des jeweiligen Arbeitsbereichs faktisch unsichtbar sein. Plattformen erweitern demgegenüber ihre potenzielle Reichweite, indem sie Informationen erschließen und miteinander verknüpfbar machen.

Suchbarkeit und Verknüpfbarkeit verändern auch die Verteilung polizeilicher Aufmerksamkeit. Leicht recherchierbare und gut strukturierte Informationen können schneller in Ermittlungen, Auswertungen oder Lagebilder einbezogen werden. Umgekehrt bleiben Sachverhalte schwerer erkennbar, wenn sie unvollständig erfasst, nicht ausreichend strukturiert oder in den zugrunde liegenden Datenmodellen nur unzureichend abbildbar sind. Datenplattformen verteilen Aufmerksamkeit somit nicht neutral. Ihre Kategorien, Suchmöglichkeiten und Verknüpfungslogiken beeinflussen, welche Zusammenhänge mit geringem Aufwand sichtbar werden und welche zusätzliche fachliche Interpretation erfordern. Besonders relevant ist dies für Ermittlungs- und Auswerteprozesse. Polizeiliche Erkenntnis entsteht häufig durch die Verbindung zunächst getrennter Informationen über Personen, Orte, Zeitpunkte, Kommunikationsbeziehungen, Spuren oder frühere Sachverhalte. Gemeinsame Datenräume können solche Verknüpfungen erleichtern. Zugleich bleibt die Aussagekraft der Ergebnisse davon abhängig, ob die zugrunde liegenden Daten fachlich zutreffend erfasst und ihre jeweiligen Kontexte berücksichtigt wurden (Calvanese et al., 2017; Ratcliffe, 2016). Die im begrifflichen Rahmen herausgearbeitete Bedeutung gemeinsamer Daten- und Bedeutungsmodelle erhält hier ihre praktische Konsequenz. Sie entscheidet mit darüber, welche kriminalistisch relevanten Beziehungen in der Plattform überhaupt belastbar darstellbar sind.

Zugriff, Verantwortung und Arbeitsteilung

Mit größerer Informationsverfügbarkeit stellt sich zugleich die Frage, wer unter welchen Voraussetzungen auf welche Daten zugreifen kann. Eine gemeinsame Plattform bedeutet nicht, dass sämtliche Informationen organisationsweit uneingeschränkt verfügbar werden. Zugriffsrechte, Rollen, Freigaben und Protokollierungen müssen rechtliche Befugnisse und organisatorische Zuständigkeiten abbilden. Diese Regelungen haben jedoch nicht nur eine datenschutzrechtliche Funktion. Sie beeinflussen auch die Arbeitsteilung innerhalb der Organisation. Wer unmittelbar auf einen benötigten Informationsbestand zugreifen darf, kann Aufgaben anders bearbeiten als jemand, der dafür zunächst eine andere Organisationseinheit einschalten muss. Berechtigungskonzepte strukturieren damit Informationswege, Bearbeitungszeiten und Verantwortlichkeiten. Technische Zugriffsgestaltung wird auf diese Weise zu einer organisatorischen Entscheidung darüber, wie Wissen innerhalb der Polizei verteilt und nutzbar gemacht wird (Marcucci et al., 2023).

Mit der erweiterten Reichweite der Daten wachsen auch die Anforderungen an ihre verantwortliche Pflege und Nutzung. Je weiter Daten über ihren ursprünglichen Erhebungskontext hinaus genutzt werden können, desto wichtiger wird die nachvollziehbare Zuordnung von Verantwortung für Datenqualität, Aktualisierung, Korrektur und Löschung. Fehlerhafte oder veraltete Informationen bleiben nicht auf ihr Ursprungssystem begrenzt, sondern können in weitere Auswertungen einfließen. Die Reichweite einer Datenplattform erhöht deshalb nicht nur den möglichen Nutzen vorhandener Informationen, sondern auch die organisatorischen Folgen mangelnder Datenqualität.

Veränderung von Zusammenarbeit

Gemeinsame Informationsräume verändern außerdem die Kooperation zwischen Dienststellen und Organisationseinheiten. Wo Daten nur lokal oder in fachlich getrennten Systemen verfügbar sind, muss Zusammenarbeit häufig über Anfragen, Aktenübermittlungen, Telefonate oder persönliche Kontakte hergestellt werden. Plattformen können einen Teil dieser Informationsbeschaffung unmittelbar in technische Recherche- und Zugriffsprozesse überführen. Gemeinsame Lagebilder und arbeitsteilige Auswertungen lassen sich dadurch schneller organisieren.

Diese Entwicklung verändert jedoch die Funktion persönlicher Abstimmung. Technischer Zugriff kann Informationswege verkürzen, ersetzt aber nicht zwangsläufig den Kontext, den erfahrene Sachbearbeiter oder andere Organisationseinheiten zu einzelnen Informationen vermitteln können. Eine in der Plattform verfügbare Information kann formal korrekt sein und dennoch interpretationsbedürftig bleiben. Effizientere Informationsverfügbarkeit und fachliche Kontextualisierung stehen daher nicht im Widerspruch, müssen aber organisatorisch miteinander verbunden werden (Phythian et al., 2024). Gerade an diesem Punkt zeigt sich die zuvor theoretisch begründete Verzahnung von Fachlichkeit und Technik in ihrer organisatorischen Konsequenz. Fachliche Expertise wird nicht dadurch entbehrlich, dass Informationen leichter verfügbar werden. Vielmehr erweitert sich ihre Bedeutung um die Bewertung von Qualität, Herkunft und Aussagekraft technisch bereitgestellter Informationen.

Führung und datenbasierte Steuerung

Auch Führungs- und Steuerungsprozesse verändern sich, wenn größere Datenbestände schneller ausgewertet und visualisiert werden können. Lageentwicklungen, regionale Schwerpunkte oder Fallzahlen lassen sich zusammenführen und für operative oder strategische Entscheidungen aufbereiten. Datenplattformen erweitern damit grundsätzlich die Möglichkeiten datenbasierter Steuerung. Je stärker Informationen quantifizierbar verfügbar sind, desto stärker können sie auch die Aufmerksamkeit in Steuerungsprozessen prägen. Was standardisiert erfasst, gezählt und visualisiert werden kann, lässt sich leichter vergleichen und in Berichts- oder Entscheidungssysteme integrieren. Qualitative Einschätzungen, unsichere Hinweise oder Kontextwissen sind demgegenüber schwerer zu formalisieren. Die Herausforderung liegt deshalb nicht darin, datenbasierte Steuerung gegen fachliche Bewertung auszuspielen, sondern die Aussagegrenzen quantifizierter Informationen sichtbar zu halten (Ratcliffe, 2016). Damit stellt sich auch die Frage nach der Rationalität datenbasierter Entscheidungen. Größere Datenmengen und systematische Auswertungen können Erkenntnisgrundlagen verbreitern, sie machen Entscheidungen jedoch nicht automatisch objektiver. Aussagekraft entsteht nur, wenn Daten vollständig genug, aktuell, korrekt zugeordnet und im jeweiligen Erhebungskontext angemessen interpretiert werden. Plattformen können bestehende Unsicherheiten nicht beseitigen. Unter ungünstigen Bedingungen können sie diese vielmehr über größere Informationsräume verbreiten oder durch aggregierte Darstellungen eine Genauigkeit suggerieren, die die Ausgangsdaten nicht besitzen (Marcucci et al., 2023).

Plattformen als Grundlage fachlicher Produktentwicklung

Gemeinsame Daten- und Infrastrukturgrundlagen verändern auch die Entwicklung fachlicher Werkzeuge. Auswertungen, Dashboards oder spezialisierte Anwendungen können darauf aufbauen, ohne für jeden neuen Bedarf erneut einen vollständig getrennten technischen Bestand zu schaffen. Der bereits eingeführte Plattformgedanke der Befähigung erhält hier eine konkrete organisatorische Dimension. Produktentwicklung kann näher an fachliche Bedarfe heranrücken, während gemeinsame technische Grundlagen erhalten bleiben (Hohpe, 2024). Low-Code- und No-Code-Ansätze können diese Entwicklung unterstützen, weil sie die Fachlichkeit stärker an der Erstellung solcher Lösungen beteiligen. Organisatorisch relevant ist dabei weniger die jeweilige Entwicklungstechnologie als die Frage, ob neue Anwendungen innerhalb der gemeinsamen Architektur entstehen. Werden eigenständige Datenbestände oder Schnittstellen aufgebaut, entsteht erneut Fragmentierung. Werden dagegen gemeinsame Datenmodelle und Plattformdienste genutzt, kann dezentrale fachliche Innovationsfähigkeit mit übergreifender technischer Anschlussfähigkeit verbunden werden (Hohpe, 2024; Viljoen et al., 2024). Plattformisierung verändert damit auch die Rollenverteilung zwischen Fachlichkeit und Technik. Fachliche Anforderungen werden nicht mehr lediglich formuliert und anschließend technisch umgesetzt. Fachliche und technische Kompetenzen müssen bereits während der Produktentwicklung enger verzahnt werden. Die organisatorische Herausforderung besteht darin, diese Zusammenarbeit zu ermöglichen, ohne Verantwortlichkeiten für Sicherheit, Datenqualität und technische Stabilität aufzulösen.

Von Zuständigkeiten zu sichtbaren Fähigkeiten

Die organisationswissenschaftliche Diskussion beschreibt eine solche Verschiebung seit längerem als mögliche Ergänzung einer primär stellenbezogenen durch eine stärker kompetenzbezogene Organisationslogik (Lawler, 1994). Eine weitergehende organisatorische Perspektive eröffnet sich, wenn Datenplattformen nicht ausschließlich Vorgangs-, Fall- oder Lagedaten abbilden. Polizeiorganisationen sind traditionell über Dienststellen, Funktionen und formale Zuständigkeiten strukturiert. Diese Ordnung bleibt für Verantwortung und Weisung unverzichtbar, macht jedoch nicht immer sichtbar, welche fachlichen, technischen oder analytischen Kompetenzen innerhalb der Organisation tatsächlich vorhanden sind.

Werden auch Rollen, Qualifikationen und Fähigkeiten strukturiert abgebildet, könnte die formale Zuständigkeitslogik um eine kompetenzbezogene Perspektive ergänzt werden. Für bestimmte Ermittlungen oder Projekte ließe sich dann nicht nur bestimmen, welche Organisationseinheit zuständig ist, sondern auch, wo die jeweils benötigten Fähigkeiten verfügbar sind. Fachwissen über bestimmte Kriminalitätsphänomene, analytische Kompetenzen, technische Spezialkenntnisse oder Sprachkenntnisse könnten gezielter in organisationsübergreifende Arbeitszusammenhänge einbezogen werden (Münter, 2023; Rashedi, 2022).

Eine solche Entwicklung würde die klassische Organisationsstruktur nicht ersetzen. Sie könnte jedoch die Fähigkeit verbessern, vorhandene Expertise jenseits formaler Stellenzuordnungen sichtbar und für konkrete Aufgaben verfügbar zu machen. Gerade bei komplexen oder dynamischen Lagen wäre dies eine zusätzliche Form organisationaler Steuerungsfähigkeit.

Voraussetzung weiterer Analyse- und Automatisierungsverfahren

Schließlich besitzen Datenplattformen eine vorgelagerte Bedeutung für KI- und Automatisierungsanwendungen. Solche Verfahren setzen strukturierte, verknüpfbare und hinreichend qualitätsgesicherte Daten voraus. Die Leistungsfähigkeit eines Analyseverfahrens kann deshalb nicht unabhängig von der zugrunde liegenden Datenarchitektur bewertet werden. Uneinheitliche Kategorien, unvollständige Informationen oder unklare Nutzungskontexte werden durch automatisierte Verarbeitung nicht beseitigt, sie können sich vielmehr in deren Ergebnissen fortsetzen oder verstärken (Marcucci et al., 2023). Für die Organisation bedeutet dies, dass die Einführung KI-basierter Verfahren nicht erst bei der Auswahl eines Algorithmus beginnt. Voraus gehen Entscheidungen darüber, welche Daten verfügbar sind, nach welchen Modellen sie strukturiert werden, wer ihre Qualität verantwortet und unter welchen Bedingungen sie miteinander verknüpft werden dürfen. Die Datenplattform bildet damit einen Teil der organisatorischen und technischen Voraussetzung, auf der spätere Automatisierungs- und Analyseverfahren aufbauen.

Zwischenfazit

Datenplattformen verändern polizeiliche Organisation nicht durch eine einzelne technische Funktion. Ihre Wirkung entsteht daraus, dass sie Informationszugänge, Sichtbarkeit, Zusammenarbeit und Möglichkeiten der Auswertung neu ordnen. Berechtigungen beeinflussen Arbeitsteilung, Datenmodelle strukturieren erkennbare Zusammenhänge, gemeinsame Informationsräume verändern Kooperation und datenbasierte Auswertungen erweitern die Möglichkeiten organisationaler Steuerung. Zugleich können Plattformen die Entwicklung fachlicher Produkte unterstützen und vorhandene Kompetenzen innerhalb der Organisation besser erschließbar machen.

Ihre organisatorische Wirkung bleibt jedoch an Voraussetzungen und Zielkonflikte gebunden. Größere Informationsverfügbarkeit erhöht die Bedeutung von Datenqualität und Verantwortlichkeit. Standardisierung kann Zusammenarbeit erleichtern, aber fachliche Besonderheiten einengen. Dezentrale Produktentwicklung kann Innovation fördern, zugleich aber neue Fragmentierung erzeugen. Datenbasierte Steuerung kann Erkenntnis verbessern, aber auch eine problematische Konzentration auf das Messbare begünstigen. Diese Spannungen sind keine Randprobleme der Plattformisierung, sondern ergeben sich unmittelbar aus ihren organisatorischen Wirkungen. Sie bilden deshalb den Ausgangspunkt des folgenden Kapitels.

Spannungsfelder der Plattformisierung: Fachlichkeit, Befähigung und Entwicklungsfähigkeit

Die organisatorischen Potenziale von Datenplattformen sind an Zielkonflikte gebunden, die sich nicht durch technische Gestaltung allein auflösen lassen. Plattformisierung verlangt Harmonisierung, weil gemeinsame Datenräume ohne verbindliche Standards, Datenmodelle und Zugriffsregeln kaum funktionsfähig sind. Zugleich darf diese Vereinheitlichung die fachliche Differenziertheit polizeilicher Arbeit nicht unangemessen reduzieren. Die zentrale

Gestaltungsaufgabe besteht deshalb darin, gemeinsame Strukturen zu schaffen, ohne jene Kontextabhängigkeit zu verlieren, auf die kriminalistische Bewertung und rechtmäßiges polizeiliches Handeln angewiesen sind.

Harmonisierung und fachliche Differenzierung

Standardisierung erhöht Anschlussfähigkeit, kann aber zugleich fachliche Besonderheiten verengen. Kategorien und Datenmodelle müssen Sachverhalte so weit vereinheitlichen, dass Informationen organisationsübergreifend nutzbar werden, zugleich aber Unterschiede, Rollenwechsel und Kontextabhängigkeiten abbilden können. Das Spannungsverhältnis besteht daher nicht zwischen Standardisierung und Fachlichkeit als solchen, sondern zwischen dem notwendigen Maß gemeinsamer Ordnung und der Offenheit für fachlich relevante Differenzierungen.

Damit wird die Qualität einer Plattform nicht daran messbar, wie viele Unterschiede sie beseitigt. Entscheidend ist vielmehr, ob sie Unterschiede dort vereinheitlicht, wo gemeinsame Strukturen erforderlich sind, und dort erhält, wo sie für die fachliche Interpretation bedeutsam bleiben. Plattformstrategie verlangt insofern selektive Harmonisierung statt möglichst umfassender Vereinheitlichung (Hohpe, 2024).

Befähigung und neue Fragmentierung

Fachliche Entwicklung soll möglichst nah an der operativen Praxis stattfinden. Plattformbasierte Entwicklungsumgebungen sowie Low-Code- und No-Code-Ansätze können dazu beitragen, Auswertungen, Workflows oder Anwendungen schneller an neue Anforderungen oder Kriminalitätsphänomene anzupassen und Fachbereiche stärker an ihrer Entwicklung zu beteiligen. Dieselbe Dezentralisierung kann jedoch erneut Fragmentierung hervorbringen. Werden außerhalb gemeinsamer Standards eigene Datenbestände, Berechtigungsmodelle oder Schnittstellen geschaffen, entsteht unter neuen technischen Bedingungen genau jene Struktur, deren Überwindung die Plattform ursprünglich ermöglichen sollte. Schnellere fachliche Entwicklung steht damit vor der Anforderung, die gemeinsame Architektur nicht erneut zu fragmentieren. Fachliche Befähigung setzt Handlungsspielräume voraus, dauerhaft tragfähig werden diese jedoch nur, wenn sie innerhalb gemeinsamer technischer und organisatorischer Leitplanken genutzt werden (Irani et al., 2023; Viljoen et al., 2024).

Stabilität und Entwicklungsfähigkeit

Plattformen müssen im laufenden Betrieb stabil und rechtssicher funktionieren und zugleich für neue fachliche Anforderungen, Datenquellen und technische Möglichkeiten offen bleiben. Zwischen diesen Anforderungen besteht ein dauerhafter Zielkonflikt. Stabilität verlangt verbindliche Standards und kontrollierte Veränderungsprozesse, Entwicklungsfähigkeit setzt voraus, dass diese Standards notwendige Anpassungen nicht dauerhaft erschweren. Gerade in föderalen und historisch gewachsenen IT-Landschaften kann deshalb kein endgültiges Zielbild alle zukünftigen Anforderungen vorwegnehmen. Plattformisierung ist

weniger als einmaliger Umbau denn als Fähigkeit zur kontrollierten Veränderung zu verstehen. Eine Architektur wäre langfristig nur begrenzt erfolgreich, wenn sie heutige Fragmentierung zwar beseitigt, sich aufgrund zu starrer Strukturen jedoch selbst zum nächsten Legacy-System entwickelt. Auch die Plattformforschung beschreibt Architektur und Governance nicht als statische Größen, sondern als miteinander gekoppelte Elemente, die sich im Zusammenspiel mit veränderten Umwelt- und Nutzungsanforderungen fortentwickeln (Hohpe, 2024; Irani et al., 2023; Tiwana et al., 2010).

Diese Frage gewinnt mit neuen Analyse- und Automatisierungsmöglichkeiten zusätzlich an Bedeutung. KI-basierte Verfahren, digitale Zwillinge oder perspektivisch agentische Systeme können neue Anforderungen an Datenmodelle, Schnittstellen, Nachvollziehbarkeit und Kontrollmechanismen erzeugen. Zukunftsfähigkeit bedeutet deshalb nicht, einzelne zukünftige Technologien bereits vollständig vorwegzunehmen. Entscheidend ist vielmehr, ob die Architektur neue Nutzungsszenarien aufnehmen kann, ohne dabei ihre fachlichen, rechtlichen und organisatorischen Grundlagen zu destabilisieren.

Governance als Verbindung der Spannungsfelder

Die drei Spannungsfelder treffen in der Governance der Plattform zusammen. Sie muss nicht nur Zugriffe oder technische Standards regeln, sondern Entscheidungen darüber ermöglichen, wo Vereinheitlichung erforderlich ist, welche fachlichen Spielräume erhalten bleiben sollen und unter welchen Bedingungen neue Anwendungen oder Datenquellen in die Plattform aufgenommen werden können.

Governance ist in diesem Verständnis keine nachträgliche Kontrollinstanz, sondern Teil der Entwicklungsfähigkeit der Plattform. Ihre Aufgabe besteht darin, fachliche Innovation, technische Stabilität, rechtliche Begrenzung und organisatorische Verantwortlichkeit dauerhaft miteinander in Beziehung zu setzen. Die Herausforderung der Plattformisierung liegt deshalb nicht darin, einen dieser Pole zu maximieren, sondern ihre Spannungen institutionell bearbeitbar zu machen.

Fazit und Ausblick

Der Wandel von der Insellösung zur Datenplattform bezeichnet mehr als eine Modernisierung polizeilicher IT. Mit der zunehmenden Entkopplung von Daten und einzelnen Fachverfahren verändert sich die Informationsordnung der Organisation selbst. Datenarchitekturen beeinflussen, welche Informationen verfügbar und verknüpfbar sind, wie Wissen zwischen Organisationseinheiten zirkuliert und auf welcher Informationsgrundlage polizeiliche Entscheidungen vorbereitet werden. Sie sind damit nicht lediglich technische Infrastruktur, sondern Bestandteil organisatorischer Gestaltung.

Die zentrale These des Beitrags lässt sich damit präzisieren: Datenplattformen entscheiden nicht selbst über polizeiliche Maßnahmen, strukturieren jedoch deren Informations- und Handlungsvoraussetzungen. Daraus folgt, dass ihre Gestaltung weder allein als technische noch ausschließlich als rechtliche Aufgabe verstanden werden kann. Fachlichkeit, Technik und Organisation müssen bereits auf der Ebene der Architektur zusammengeführt werden.

Der Übergang zur Plattformlogik löst die mit fragmentierten Informationslandschaften verbundenen Probleme dabei nicht automatisch. Gemeinsame Datenräume schaffen neue Möglichkeiten der Informationsnutzung, erhöhen aber zugleich die Anforderungen an Datenqualität, Verantwortlichkeit, Governance und fachliche Interpretation. Plattformisierung ist deshalb kein Endzustand, sondern eine dauerhafte Organisationsaufgabe. Ihr Erfolg hängt wesentlich davon ab, ob Harmonisierung und fachliche Differenzierung, zentrale Standards und dezentrale Befähigung sowie technische Stabilität und kontinuierliche Weiterentwicklung miteinander verbunden werden können.

Diese Fähigkeit wird mit zunehmender Bedeutung datenintensiver Analyse- und Automatisierungsverfahren weiter an Gewicht gewinnen. KI-basierte Anwendungen, digitale Zwillinge oder agentische Systeme können nur so belastbar sein wie die Datenarchitekturen, auf denen sie aufbauen. Die entscheidende Zukunftsfrage lautet daher weniger, welche einzelne Technologie als Nächstes eingeführt wird. Maßgeblich ist, ob die Polizei eine Informationsarchitektur entwickelt, die neue technische Möglichkeiten aufnehmen kann, ohne fachliche Urteilskraft, Verantwortlichkeit und rechtsstaatliche Kontrolle zu schwächen. Der eigentliche Maßstab einer polizeilichen Datenplattform liegt damit nicht in maximaler Zentralisierung oder technischer Leistungsfähigkeit, sondern in ihrer Fähigkeit, polizeiliche Handlungsfähigkeit mit organisationaler Lern- und Entwicklungsfähigkeit zu verbinden.

Referenzen

Bundesministerium des Innern und für Heimat. (2023). P20—Auf dem Weg zu einer gemeinsamen, digitalen und vernetzten Polizei. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI23004.html

Calvanese, D., De Giacomo, G., Lembo, D., Lenzerini, M., & Rosati, R. (2017). Ontology-Based Data Access and Integration. In L. Liu & M. T. Özsu (Hrsg.), Encyclopedia of Database Systems (S. 1–7). Springer New York. https://doi.org/10.1007/978-1-4899-7993-3_80667-1

De Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. Journal of Information Technology, 33(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

Gieß, A., Möller, F., Schoormann, T., & Otto, B. (2023). Design Options for Data Spaces. Proceedings of the 31st European Conference on Information Systems (ECIS 2023). https://aisel.aisnet.org/ecis2023_rp/287/

Hohpe, G. (2024). Platform Strategy: Innovation Through Harmonization. Leanpub.

Hollywood, J., Boon, J. E. J., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015). High-Priority Information Technology Needs for Law Enforcement. RAND Corporation.

Innenministerkonferenz. (2016). Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit.

Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. Government Information Quarterly, 40(1), 101784. https://doi.org/10.1016/j.giq.2022.101784

Lawler, E. E. (1994). From job-based to competency-based organizations. Journal of Organizational Behavior, 15(1), 3–15. https://doi.org/10.1002/job.4030150103

Marcucci, S., Alarcón, N. G., Verhulst, S. G., & Wüllhorst, E. (2023). Informing the Global Data Future: Benchmarking Data Governance Frameworks. Data & Policy, 5, e30. https://doi.org/10.1017/dap.2023.24

Münter, M. T. (Hrsg.). (2023). Wie verändern Daten Unternehmen? Strategie und Organisation für eine datengetriebene Welt (1. Auflage). UVK Verlag. https://doi.org/10.24053/9783739882246

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science, 3(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

Phythian, R., Kirby, S., & Swan-Keig, L. (2024). Understanding how law enforcement agencies share information in an intelligence-led environment: How operational context influences different approaches. Policing: An International Journal, 47(1), 112–125. https://doi.org/10.1108/PIJPSM-06-2023-0073

Rashedi, J. (2022). Das datengetriebene Unternehmen: Erfolgreiche Implementierung einer data-driven Organization. Springer Gabler.

Ratcliffe, J. H. (2016). Intelligence-Led Policing (2. Aufl.). Routledge. https://doi.org/10.4324/9781315717579

Star, S. L., & Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information Systems Research, 7(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. Information Systems Research, 21(4), 675–687. https://doi.org/10.1287/isre.1100.0323

Viljoen, A., Hein, A., Nguyen, J., & Krcmar, H. (2024). Governing Citizen Development to Address Low-Code Platform Challenges. MIS Quarterly Executive, 305–324. https://doi.org/10.17705/2msqe.00100

Digitale Fahrzeugdaten als Entwicklungslinie moderner Polizeitechnik – Rechtliche Leitplanken und praxisnahe Nutzung im digitalen Zeitalter

Andreas Mehlich und Kilian L. Scholz

Wenngleich von Zeit zu Zeit unter Effizienzgesichtspunkten diskutiert wird, die Aufgaben der Polizei bei der Verkehrsunfallaufnahme zu reduzieren (Melchers, 1994, S. 4) oder gebührenrechtlich neu zu bewerten (Der Tagesspiegel, 2010), gehört die Aufnahme von Verkehrsunfällen weiter zum festen Aufgabenspektrum der Landespolizeien. Die rechtliche Notwendigkeit hoheitlicher Unfallaufnahme erwächst aus der polizeirechtlichen Aufgabenzuweisung zum Schutz privater Rechte (z. B. § 1 PolG NRW, § 1 ASOG Bln.), denn regelmäßig ergeben sich bei Verkehrsunfällen zumindest zivilrechtliche Schadensersatzansprüche, insb. aus §§ 7, 16 StVG, § 823 BGB (Grüneberg, 2023, Rn. 1). Verkehrsunfälle sind überwiegend die Folge einer Missachtung verkehrsrechtlicher Vorschriften (Schlanstein, 2016, S. 201), was die Aufgabenzuweisung der Polizei zur Verfolgung von Ordnungswidrigkeiten eröffnet (§ 53 OWiG). Spätestens bei Verkehrsunfällen mit Personenschäden steht regelmäßig der Verdacht einer Straftat, etwa fahrlässige Körperverletzung (§ 229 StGB), im Raum (König, 2023, Rn. 1), sodass die Polizei im Wege ihrer Strafverfolgungspflicht aus § 163 Abs. 1 StPO zur Beweissicherung berufen ist (Köhler, 2025, § 110 Rn. 27).

Die Sicherung der Unfallszene, d. h. der Gesamtheit des Unfallgeschehens (vgl. Weber, 2023, 21. A. Rn. 1), ist die Grundlage jeder Verkehrsunfallaufklärung und Voraussetzung zur Bestimmung von Verantwortlichkeiten nach dem Verkehrshaftungs-, Straf- und Ordnungswidrigkeitenrecht. Informationen über den Unfallhergang sind ferner relevant für die Prävention durch Verkehrssicherheitsarbeit und Verkehrsunfallforschung (Fothen & Böhm, 2026, S. 45, 48), gehen in ihrem Nutzen also über das konkrete Unfallszenario hinaus.

Es gilt: Je genauer und umfassender die Informationen über eine Unfallszene sind, desto eher kann eine Rekonstruktion des Unfallgeschehens und eine Bestimmung der Unfallursachen gelingen. Die Verkehrsunfallaufnahme und die Ursachenermittlung bedeuten früher wie heute datenbasierte Informationsgewinnung und -verarbeitung. Die klassische polizeiliche Verkehrsunfallaufnahme beschränkte sich dabei vorrangig auf außerhalb der Fahrzeuge befindliche Informationen (etwa Lichtbilder, Reifenspuren, physische Schadensbilder am Fahrzeug, Verletzungsbilder von Unfallbeteiligten, Zeugenaussagen). Durch die Transformation von Kraftfahrzeugen zu vernetzten, cyberphysischen Systemen wurden Kraftfahrzeuge mehr und mehr zu „mobilen Datenspeichern“. So begann mit der Einführung elektronischer Steuergeräte (ECUs) in den 1970er Jahren, insbesondere für die Motorsteuerung und Zündung, der Übergang vom rein mechanischen zum elektronisch unterstützten Fahrzeug (Eisenberg, 2017, Rn. 1939; Reif, 2016, S. 5).

In den 1980er Jahren folgten weitere Systeme wie Antiblockiersysteme (ABS) und erste Bordcomputer, während sich in den 1990er Jahren die Digitalisierung durch Airbagsysteme, elektronische Stabilitätsprogramme (ESP) und vernetzte Steuergeräte deutlich ausweitete (Mildner et al., 2024, S. 49). Seit den 2000er Jahren wird das Fahrzeug

zunehmend durch umfassende Vernetzung, Sensorik und softwaregestützte Funktionen geprägt (Mildner et al., 2024, S. 100–102). Die hierdurch anfallenden Fahrzeugdaten eröffnen als digitale Spuren zahlreiche Ermittlungsansätze (Eisenberg, 2017, Rn. 1939).

Schon bei quantitativer Betrachtung der bundesweiten Unfallstatistik der Hauptverursacher von Unfällen mit Personenschaden für die Jahre 2021 bis 2024 (Statistisches Bundesamt, 2025) zeigt sich eine deutliche Dominanz von Kraftfahrzeugen als Hauptverursacher. Dies bedeutet auch, dass bei Verkehrsunfällen mit Personenschaden die Möglichkeit besteht, die Ermittlungen auf die dort vorliegenden digitalen Fahrzeugspuren zu erstrecken, sodass sich ein großes Einsatzpotenzial ergibt.

Gegenstand dieses Beitrags ist die Betrachtung digitaler Kraftfahrzeugdaten als moderner polizeitechnischer Ermittlungsansatz speziell im Kontext von Verkehrsunfällen. Angesichts der Vielzahl der technischen Komponenten in modernen Kraftfahrzeugen (Cinar, 2025, S. 74; Mildner et al., 2024, S. 104), die für Ermittlungszwecke herangezogen werden könnten, soll der Schwerpunkt auf dem sog. Event Data Recorder (EDR) liegen. Bei dem EDR handelt es sich um einen Datenspeicher im Fahrzeug, der ereignisbezogen (Unfallereignis) bestimmte Fahr- und Fahrzeuginformationen aufzeichnet, aus denen eine Rekonstruktion des Unfallhergangs möglich ist (Brockmann & Nugel, 2024, S. 661). Diese Daten können neben der Spurenerhebung im Wege der klassischen Verkehrsunfallaufnahme zumindest ergänzende Beweisrelevanz entfalten (Schmid & Wessels, 2017, S. 357–358), sind jedoch besonders bedeutsam bei Unfallereignissen mit im Übrigen fehlender oder unzureichender Spurenzeichnung (Brockmann & Nugel, 2024, S. 661).

Während der EDR im Schrifttum bislang, soweit zu übersehen, vorrangig aus technischer, datenschutzrechtlicher sowie zivilrechtlicher Perspektive betrachtet wurde, verfolgt die hiesige Darstellung einen ganzheitlichen Ansatz, der den EDR zunächst im Gesamtsystem digitaler Fahrzeugarchitektur einordnet, sodann die technische Architektur des EDR darstellt, auf Grundlage dieser Erkenntnisse den ermittlungspraktischen Mehrwert für die polizeiliche Ermittlungstätigkeit diskutiert sowie diesbezüglich rechtspolitische Impulse aufzeigt. Weiter erfolgt eine rechtliche Einordnung mit Schwerpunkt auf die für die polizeilichen Ermittlungen relevanten strafprozessualen Zugriffsgrundlagen.

Die Datenwelt moderner Fahrzeuge

Das moderne Kraftfahrzeug ist heute ein mobiles Datendepot und erzeugt in kurzer Zeit erhebliche Datenmengen. Dabei können ohne Weiteres Größenordnungen von etwa 25 Gigabyte pro Stunde erreicht werden (Wiebe et al., 2023, S. 11; Freymann, 2025, Einl. Rn. 97 m. w. N.), sodass der Bezeichnung „rollender Computer“ (Weichert, 2016, S. 361) uneingeschränkt zuzustimmen ist. Die erfassten Daten weisen unterschiedliche Ursprünge und Funktionen auf und lassen sich typologisch ordnen, was zugleich das „Bermudadreieck des digitalen Zeitalters“ (Mehlich & Härter, 2025, S. 214) sichtbar macht.

Unter fahrzeuginternen Daten sind sämtliche Informationen zu verstehen, die unmittelbar im Fahrzeug selbst erzeugt und verarbeitet werden (transformationswissen BW, 2021, S. 4). Hierzu zählen insbesondere Sensor-, Betriebs- und Zustands-

daten, etwa zu Geschwindigkeit, Bremsverhalten oder technischen Funktionen. Einen Sonderfall bildet der EDR, der bestimmte Parameter kurz vor und während eines Unfallereignisses aufzeichnet. Davon zu unterscheiden sind umfeldbezogene Daten, die nicht das Fahrzeug selbst, sondern dessen Umgebung betreffen (v. Schönfeld, 2015, S. 618). Diese werden über Kameras, Radar- oder Lidarsysteme erhoben und dienen vor allem der Erfassung von Verkehrssituationen, Hindernissen oder anderen Verkehrsteilnehmern. Sie bilden die Grundlage für Assistenzsysteme und zunehmend auch für automatisierte Fahrfunktionen.

Als vernetzte Daten (Connected Car Data) werden hingegen solche Informationen bezeichnet, die im Rahmen der Kommunikation des Fahrzeugs mit seiner Umgebung entstehen oder übertragen werden (vgl. Kühne, 2022, Kap. A. Rn. 13). Hierunter fallen insbesondere Telematikdaten sowie sogenannte V2X-Daten, wie z. B. Daten der Verkehrsinfrastruktur oder digitaler Dienste. Sie ermöglichen etwa Echtzeitinformationen zum Verkehrsfluss oder sicherheitsrelevante Warnmeldungen. Unter dem Begriff V2X (vehicle-to-everything) werden übergreifend die Einzelkomponenten des vernetzten Fahrens zusammengefasst, die die Kommunikation zwischen Fahrzeugen (V2V – vehi-cle-to-vehicle), mit der Infrastruktur (V2I – vehicle-to-infrastructure), mit Fußgängern (V2P – vehicle-to-pedestrian) sowie mit externen Endgeräten (V2D – vehicle-to-device) beschreiben (Seckelmann, 2024, 2.7.1 Rn. 6 m. w. N.).

Schließlich können diese Datenarten begrifflich in Dienste- und Nutzungsdaten sowie in fahrzeugbezogene Daten unterteilt werden (Tinnefeld, 2025, Kap. 27 Rn. 2). Diese dienen als vereinfachte Sammelkategorien und sind insbesondere im rechtlichen Kontext anschlussfähig, da sie unterschiedliche Datenquellen bündeln, ohne sich auf technische Details festzulegen.

Der Event Data Recorder als Schlüsseltechnologie moderner Car-Forensik

Die fortschreitende Digitalisierung moderner Fahrzeuge verändert nicht nur die technische Struktur des Kraftfahrzeugs selbst, sondern eröffnet zugleich neue Möglichkeiten der polizeilichen Verkehrsunfallarbeit.

Das vernetzte Fahrzeug als Ausgangspunkt

Die Entwicklung des Kraftfahrzeugs vom rein mechanischen Fortbewegungsmittel zum vernetzten, datengestützten System bildet die technische Grundlage für die heutige Bedeutung digitaler Fahrzeugdaten. Mit jeder neuen Modellgeneration werden zusätzliche technische Systeme integriert. Hierzu zählen etwa Notrufsysteme, Fahrassistenzfunktionen, Einrichtungen zur Unfalldokumentation, verschiedene Warnsysteme, Ansätze autonomer Fahrzeugsteuerung, die Analyse von Verkehrsflüssen sowie Unterhaltungs- und Informationsangebote, Telekommunikationsfunktionen sowie automatisierte Zustandsüberwachungen des Fahrzeugs (v. Schönfeld, 2015, S. 617).

Diese Transformation hat die Car-Forensik als eigenständiges Handlungsfeld erst möglich gemacht. Während Unfallrekonstruktion traditionell auf physischen Spuren, Zeugenaussagen und modellhaften Berechnungen beruht, entstehen heute im Fahrzeug selbst unsichtbare Spuren, die das Unfallgeschehen zeitlich und inhaltlich hochaufgelöst abbilden

können. Dennoch wird dieses Potenzial in der polizeilichen Praxis bislang nur punktuell ausgeschöpft. Pionierarbeit leistete das Projekt „ProDigi – Sicherung digitaler Fahrzeugspuren zur Verkehrsunfallaufnahme“ des Landesamts für Zentrale Polizeiliche Dienste (LZPD) in Nordrhein-Westfalen, das von März 2017 bis Juni 2019 durchgeführt wurde und grundlegende Ansätze für die systematische Sicherung und Auswertung digitaler Fahrzeugdaten im Rahmen der Verkehrsunfallaufnahme entwickelte (vgl. Paul & de Valck, 2023, S. 1587 m. w. N.). Die Landespolizei Baden-Württemberg hat im Jahr 2021 insgesamt 25 Auslesegeräte beschafft (MI BW, 2021). Niedersachsen erprobt seit 2023 mit dem Projekt „Digitale Verkehrsunfallspuren“ eine EDR-gestützte Unfallauswertung, die ab 2026 den landesweiten Standard darstellen soll (Die Zeit, 2025).

Damit ist bereits der erste Schritt auf dem Weg von der klassischen Unfallaufnahme hin zur datenbasierten Unfallrekonstruktion vollzogen. Dabei handelt es sich um einen Entwicklungsschritt, der sich durchaus als nichts weniger als ein argonautischer Aufbruch der modernen Verkehrsunfallforensik bezeichnen lässt. Gleichwohl mangelt es vielfach noch an standardisierten Verfahren, ausreichender technischer Ausstattung und rechtlicher Sensibilisierung, sodass ein systematischer Umgang mit digitalen Fahrzeugdaten auch zehn Jahre später noch in den Kinderschuhen steckt.

Technische Grundstruktur und Funktionslogik des EDR

Beim EDR handelt es sich nicht um ein eigenständiges technisches Gerät, sondern um einen Bestandteil des Airbag-Steuergeräts (Burg, 2017, S. 827), der seit rund zehn Jahren in nahezu allen modernen Neufahrzeugen verbaut ist. Ursprünglich wurde er entwickelt, um die ordnungsgemäße Funktion der Airbags nachvollziehen zu können, wobei zunächst nur die für deren Auslösung relevanten Parameter gespeichert wurden (Mehlich & Härter, 2026, S. 39). Im Laufe der Zeit wurde der Umfang der erfassten Daten jedoch deutlich erweitert. Technisch verfügt der EDR über einen Ringspeicher, der kontinuierlich Daten aufzeichnet, diese aber nur bei Eintritt eines besonderen Ereignisses (sog. „Event“) speichert, während sie ansonsten fortlaufend überschrieben werden (Fothen et al., 2020, S. 284). Kommt es zu einem solchen Ereignis, werden die Daten aus einem kurzen Zeitraum vor und nach dem Ereignis in einen Festspeicher übertragen und dort gesichert. Nach dem Ausschalten der Zündung bleiben daher grundsätzlich nur diejenigen Daten erhalten, die zuvor anlässlich eines Ereignisses im Festspeicher abgelegt wurden (Freymann, 2025, Einl. Rn. 98).

Inhaltlich wird zwischen sog. „deployment events“ und „non deployment events“ unterschieden (Brockmann & Nugel, 2024, S. 661). „Deployment events“ liegen vor, wenn Rückhaltesysteme wie Airbags oder Gurtstraffer ausgelöst werden. Die hierbei gespeicherten Daten bleiben dauerhaft erhalten und können nicht überschrieben werden. Demgegenüber erfassen „non deployment events“ insbesondere starke Geschwindigkeitsänderungen, ohne dass Sicherheitssysteme ausgelöst werden. Nach europarechtlichen Regelungen werden Geschwindigkeitsänderungen von mindestens 8 km/h innerhalb von 150 Millisekunden erfasst (Art. 2 Abs. 1 lit. a Verordnung (EU) 2021/1215 unter Verweis auf UN-Regelung Nr. 160), und zwar sowohl bei Verzögerungen als auch bei Beschleunigungen in Längs- und Querrichtung. Solche Werte werden typischerweise bei Beinaheunfällen oder riskanten Fahrmanövern erreicht, ohne dass es zwingend zu einer Kollision kommen muss. Hier lassen sich insbesondere aus strafrechtlicher Sicht relevante Informationen zu gefährlichen Fahrmanövern oder

Beinaheereignissen gewinnen, etwa zu relativ leichten Anstößen gegen vulnerable Verkehrsteilnehmende. Diese Ereignisse werden gespeichert, können jedoch im Unterschied zu „deployment events“ durch neuere Einträge überschrieben werden.

Typischerweise umfasst die gespeicherte Sequenz fünf Sekunden vor und bis zu zwei Sekunden nach dem auslösenden Ereignis (Brockmann & Nugel, 2024, S. 661). Dieses Zeitfenster erscheint auf den ersten Blick kurz, deckt aber bei realistischer Betrachtung gerade die entscheidenden Momente ab, in denen das Verhalten der Fahrzeugführenden unfallursächlich wird. In der überwiegenden Zahl der Fälle konzentrieren sich die relevanten Reaktions- und Kollisionsvorgänge auf die letzten zwei bis drei Sekunden vor dem Unfall (Burmann & Schmedding, 2015, § 4 Rn. 1). Insofern ist die Speicherlogik des EDR – wenngleich zufällig – auf die polizeilichen Erkenntnisinteressen zugeschnitten, ohne den Datenbestand unnötig auszuweiten. Damit folgt sie dem Prinzip der Datensparsamkeit.

Umfang und Qualität der aufgezeichneten Daten

Welche Datensätze im EDR gespeichert werden, ist unionsrechtlich vorgegeben. Die Verordnung (EU) 2019/2144 dient der harmonisierten Umsetzung der Anforderungen aus der UN-Regelung Nr. 160 (vgl. Erwägungsgrund 4 Verordnung (EU) 2022/545 und Beschluss 97/836/EG). Hierin werden als verbindliche Mindestanforderungen derzeit mehr als 45 standardisierte Datenelemente, einschließlich ihrer Abtastraten, Genauigkeit und Auflösung, festgelegt. Hierzu zählen unter anderem Geschwindigkeit, Fahrpedalstellung, Bremsstatus, Airbagauslösung, Sicherheitsgurtstatus sowie kollisionsbedingte Geschwindigkeitsänderungen. Darüber hinaus werden weitere fahrdynamische Parameter, Systemzustände und Ereignismerkmale erfasst. Die tatsächliche Datentiefe geht häufig über diese Mindeststandards hinaus, da Hersteller zusätzliche Daten nach eigenem Ermessen speichern können. Theoretisch ist es daher möglich, nahezu alle im Fahrzeug anfallenden Daten zu erfassen, wobei allerdings Ton- und Bildaufzeichnungen ausgeschlossen sind.

Für die polizeiliche Unfallrekonstruktion gewinnen diese Daten insbesondere dann an Bedeutung, wenn sie den einzelnen Phasen eines Unfallgeschehens zugeordnet werden können. Die hierdurch eröffneten Beweismöglichkeiten beschränken sich dabei nicht allein auf die allgemeine Rekonstruktion des Unfallhergangs, sondern ermöglichen auch Feststellungen zu Einzelvorgängen wie Anstoßwinkel, Kollisionsdauer, mittlere Anstoßbeschleunigung und Auslaufverhalten (Hamann, 2025, § 22 Rn. 85). Dank des GPS-Sensors werden Positionsdaten ebenso wie die Zeit und die zurückgelegte Wegstrecke exakt gespeichert.

Pre-Crash-Daten

Die Pre-Crash-Daten bilden den technisch wie rechtlich besonders aussagekräftigen Abschnitt der Datenerfassung, da sie das Verhalten des Fahrzeugs und indirekt auch des Fahrers unmittelbar vor dem Unfall abbilden (vgl. Paul & de Valck, 2023, S. 1588), wobei die Aufzeichnung in kurzen Intervallen erfolgt. In dieser Phase entstehen die entscheidenden Anknüpfungstatsachen für die Rekonstruktion des Unfallhergangs, da sich hier zeigt, ob und wie auf eine erkannte Gefahr reagiert wurde.

Typischerweise lassen sich aus den Pre-Crash-Daten der Geschwindigkeitsverlauf, die Stellung des Fahrpedals, eine etwaige Bremsbetätigung, der Lenkwinkel sowie die Aktivität fahrdynamischer Regelsysteme wie ABS oder ESP ablesen (Berg, 2025, S. 621–624). Daraus kann beispielsweise rekonstruiert werden, ob eine Person versucht hat zu bremsen oder auszuweichen, ob eine konstante Geschwindigkeit beibehalten wurde oder ob kurz vor der Kollision noch beschleunigt wurde. Auch das Ausbleiben bestimmter Reaktionen kann dabei von erheblicher Aussagekraft sein, etwa wenn keinerlei Bremsbetätigung erfolgt ist.

In-Crash-Daten

Die In-Crash-Daten (bzw. Eventdaten) sind die Fahrzeugdaten, die während des eigentlichen Aufpralls aufgezeichnet werden, also in der Kollisionsphase selbst (Appel et al., 2002, S. 18). Dazu zählen typischerweise Informationen wie Änderungen der Geschwindigkeit, Beschleunigungen, Auslösezeitpunkte von Airbags und der Status von Sicherheits- und Rückhaltesystemen. Darüber hinaus wird dokumentiert, um welche Art von Ereignis es sich handelt, wie viele solcher Ereignisse vorliegen und wie viel Zeit zwischen ihnen vergangen ist (Kreutner & Nugel, 2023, S. 179 Rn. 11).

Post-Crash-Daten

Die Post-Crash-Daten erfassen die Phase der sich unmittelbar anschließenden Auslaufbewegung des Fahrzeugs. Sie dokumentieren damit vor allem die physikalischen Auswirkungen des Unfallgeschehens und ermöglichen eine präzise Einordnung von Aufprallintensität, Bewegungsrichtung und Energieumsetzung. Im Mittelpunkt stehen dabei insbesondere die kollisionsbedingten Geschwindigkeitsänderungen (Delta v) in Längs- und Querrichtung, deren zeitlicher Verlauf sowie die dabei auftretenden Beschleunigungen (Kreutner & Nugel, 2023, S. 179 Rn. 11). Ergänzend werden häufig auch Rotationsbewegungen, etwa in Form von Roll- oder Gierwinkeln, erfasst.

Diese Daten erlauben Rückschlüsse darauf, wie heftig die Kollision war, aus welcher Richtung die Krafteinwirkung erfolgte und wie sich das Fahrzeug infolge des Aufpralls weiterbewegt hat. Sie sind damit von besonderer Bedeutung für die technische Rekonstruktion des Unfallgeschehens, etwa im Hinblick auf Kollisionskonstellationen, Anstoßpunkte oder die Dynamik der beteiligten Fahrzeuge. Auch lassen sich aus den gemessenen Belastungen Hinweise auf mögliche Verletzungsabläufe ableiten. Gerade in Ergänzung zu den Pre-Crash-Informationen entsteht ein vollständigeres Bild von Ablauf und Intensität des Unfallgeschehens.

Fehlerquellen

Die Datenqualität des EDR darf nicht im Sinne absoluter Fehlerfreiheit missverstanden werden. Die verbauten Sensoren und das Messverfahren sind primär auf die Steuerung und Überwachung des Fahrzeugs ausgelegt, nicht auf die forensische Detailrekonstruktion. Es können neben Messungenauigkeiten Konstellationen auftreten, in denen bestimmte Ereignisse nicht aufgezeichnet werden, etwa bei sehr geringfügigen Kollisionen oder bei Kollisionen mit ungeschützten Verkehrsteilnehmern, die die Auslöseschwellen nicht er-

reichen, was typischerweise bei Kollisionen mit Fußgängerinnen und Fußgängern oder Radfahrenden der Fall sein kann, wenn keine relevante Geschwindigkeitsänderung eintritt (Dürnberger & Kreutner, 2017, S. 340).

Weiter können Messungenauigkeiten einzelner Sensoren oder programmbedingte fehlerhafte Umrechnungen dazu führen, dass bestimmte Parameter nicht ohne Weiteres mit der Realität übereinstimmen. Ebenso können Fahrzustände wie in der Luft befindliche durchdrehende Räder oder Mängel an der Bereifung die gemessene Geschwindigkeit verfälschen (Mehlich & Härter, 2026, S. 49–51). Auch das Risiko von Datenverlust bei Werkstattaufenthalten oder infolge unsachgemäßer Bergung beschädigter Fahrzeuge besteht. Aus forensischer Sicht ist daher ein standardisiertes Vorgehen unerlässlich. Dazu gehören klare Vorgaben zur Sicherstellung und Bergung, der frühzeitige Abgleich von Fahrzeugzeit und realer Zeit, die sorgfältige Dokumentation aller Veränderungen am Fahrzeug sowie der Einsatz geeigneter Auslesetechnik durch geschultes Personal. Ferner bedarf es einer fachkundigen Interpretation der Daten, die auch die herstellerspezifischen „Data Limitations“ einbezieht.

Verbreitung und rechtlicher Rahmen der EDR-Ausstattung

Mit der europäischen Typgenehmigungs-Regulierung (Verordnung (EU) 2019/2144) ist der EDR von einer freiwilligen Option einzelner Hersteller zu einer flächendeckend eingeführten Pflichtausstattung geworden. Seit Juli 2022 müssen alle neuen Fahrzeugtypen mit einem EDR ausgerüstet sein, seit Juli 2024 gilt dies für alle zugelassenen Neufahrzeuge der Fahrzeugklassen M1 und N1. In weiteren Schritten werden auch schwere Nutzfahrzeuge, Busse und andere Fahrzeugkategorien einbezogen, sodass in absehbarer Zeit der überwiegende Teil der europäischen Fahrzeugflotte über einen EDR verfügen wird.

Damit wächst das praktisch verfügbare Datenvolumen in erheblichem Umfang. Für die Polizei bedeutet das, dass sich die EDR-Nutzung von einem Spezialinstrument für Einzelfälle zu einem regulären Bestandteil der Unfallaufnahme und -rekonstruktion entwickeln kann. Die Auslesetechnik mittels CDR-Software über eine einheitliche OBD2-Schnittstelle ist bereits etabliert (Burg, 2017, S. 829–831). Sie erlaubt sowohl ein Auslesen im Fahrzeug als auch aus ausgebauten Steuergeräten (Paul & de Valck, 2023, S. 1596).

Zwischenfazit: EDR als prototypische Polizeitechnik des 21. Jahrhunderts

Der Event Data Recorder steht sinnbildlich für die Entwicklung moderner Polizeitechnik im 21. Jahrhundert. Er verbindet technische Innovation, organisatorische Anpassungsbedarfe und rechtliche Herausforderungen in einem Feld, das zunehmend an Bedeutung für die tägliche Verkehrssicherheitsarbeit gewinnt. Die durch ihn eröffneten Ermittlungs- und Beweismöglichkeiten markieren einen qualitativen Sprung in der Aufklärung von Verkehrssachverhalten und berühren zugleich grundlegende Fragen der Verantwortung zwischen staatlichen und privaten Akteuren.

Strafprozessuale Zugriffsgrundlagen und rechtliche Problemfelder

Die im EDR abgelegten Datensätze sind im IT-forensischen Sinne digitale Spuren, weil sie auf Daten (hier: ereignisbezogenen Fahrzeugdaten als unfallbezogene Informationen, Art. 3 Nr. 13 Verordnung (EU) 2019/2144) beruhen und in einem Computersystem gespeichert sind (Marschall, 2019, S. 92). Digitale Spuren setzen regelmäßig digitalforensische Analyseverfahren voraus, damit aus ihnen ermittlungsrelevante Erkenntnisse für das Strafverfahren gewonnen werden können (Jahn & Brodowski, 2020, S. 70). Ist dies der Fall, kann von digitalen oder elektronischen Beweismitteln gesprochen werden (Jahn & Brodowski, 2020, S. 70). Sie sind keine eigene Beweiskategorie, sondern in die bestehende Systematik der Beweismittel der StPO einzuordnen.

Im Bereich der IT-Forensik ist heute ein dreistufiges Vorgehen nach dem S-A-P-Modell (Secure-Analyse-Process) anerkannt (Marschall, 2019, S. 97; Morgenstern, 2011, S. 204). Danach stellt die Sicherung von Daten den Beginn dar, bevor die Auswertung und Interpretation erfolgen kann und schließlich im letzten Schritt die ermittlungsrelevante Präsentation ausgewerteter Daten möglich wird (Jahn & Brodowski, 2020, S. 70; Marschall, 2019, S. 103). Um die sich in der Ermittlungspraxis stellenden Rechtsfragen strafprozessualer Natur prozessorientiert und damit praxisnah abzubilden, folgt die rechtliche Darstellung dem S-A-P-Modell (vgl. Raab-Düsterhöft, 2024, S. 19–21). Denn auf den einzelnen Stufen stellen sich unterschiedliche Eingriffs- und Beweisfragen.

Sichern (Secure)

Die erste Stufe bildet die Sicherung der EDR-Daten. Strafprozessual ist bezüglich der Sicherung digitaler Daten näher zu differenzieren, ob es sich um Daten handelt, die bereits gespeichert sind (z. B. physische Sicherung von Datenträgern), über Telekommunikationsnetze übermittelt werden (z. B. Überwachung laufender Telekommunikation) oder erst noch erhoben werden sollen (z. B. Beobachtung einer Person in Form einer Standortüberwachung), weil je nach Zielrichtung andere Rechtsgrundlagen heranzuziehen sind (Jahn & Brodowski, 2020, S. 71). EDR-Daten betreffen regelmäßig im Fahrzeug gespeicherte Daten (Reid, 2024, 2.8.2. Rn. 8), womit die erste Fallgruppe einschlägig ist. Von forensischem Interesse sind hierbei die Daten, die über die temporäre Speicherung im Ringspeicher des EDR bei einem relevanten Ereignis in den Festspeicher abgelegt werden und auch nach dem Ausschalten der Zündung persistent sind (Fothen et al., 2020, S. 285).

Insofern sollte durch die Verfolgungsbehörden eine Sicherung der Datensätze des EDR-Festspeichers i. d. R. physisch am Fahrzeug erfolgen, optimalerweise an Ort und Stelle des Unfallereignisses, um einen Beweismittelverlust und damit die Verdunkelung der Sache zu verhüten, wie es § 163 Abs. 1 S. 1 StPO als Aufgabenzuweisung (nicht als einschlägige Eingriffsbefugnis) normiert.

Weiterhin ist strafprozessual zwischen der offenen und verdeckten Sicherung zu unterscheiden (Jahn & Brodowski, 2020, S. 71). In aller Regel wird nur eine offene Sicherung der (retrograden) EDR-Daten in Betracht kommen, weil auch die übrige Verkehrsunfallaufnahme

durch die (uniformierte) Verkehrspolizei offen erfolgt. Für eine verdeckte Sicherung wird typischerweise kein Raum verbleiben, da regelmäßig kein Grund für eine grundrechtsintensivere verdeckte Erhebung vorliegen wird.

Die StPO enthält gegenwärtig keine EDR-spezifische spezialgesetzliche Befugnisnorm für den offenen Zugriff auf lokale (physische) Datenspeicher oder gar eine spezialgesetzliche Zugriffsnorm für fahrzeugbezogene Datenspeicher. Allerdings ist eine Befugnis für die hoheitsrechtliche Sicherung des EDR-Speichers erforderlich, weil die Maßnahme verfassungsrechtlich jedenfalls das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG betrifft (BVerfGE 84, 212, 226). Ferner ist bereits unionsrechtlich nach Art. 4 Abs. 1 lit. a, Art. 8 Richtlinie (EU) 2016/680 für staatliche Eingriffsmaßnahmen in das datenschutzrechtliche Unionsgrundrecht (vgl. Art. 8, 51 GrCh) eine nationalstaatlich hinreichende Kodifizierung einfachrechtlicher Befugnisse erforderlich.

Dies gilt auch für EDR-Daten. Entgegen der Formulierung in Erwägungsgrund 13 zu Verordnung (EU) 2019/2144, der bei der ereignisbezogenen Datenaufzeichnung in Kraftfahrzeugen von „wichtigen, anonymisierten Fahrzeugdaten" spricht und davon ausgeht, dass „anhand dieser Daten keine Identifizierung des Nutzers oder Halters eines bestimmten Fahrzeugs möglich ist", wird bei EDR-Daten zumindest für die Strafverfolgungsbehörden ein Personenbezug dieser Datensätze zu bejahen sein. Denn angesichts der im Rahmen der Verkehrsunfallaufnahme ebenfalls erfolgenden Erfassung der Personalien von Fahrzeughalter und Fahrzeugführer sowie des Kennzeichens (BVerfGE 120, 378, 399) wird eine Verbindung zwischen diesen Datensätzen ersichtlich (Fothen et al., 2020, S. 286). Damit ist spätestens unter Berücksichtigung des den EDR-Daten zu entnehmenden Fahrverhaltens von (indirekt) personenbezogenen Daten i. S. d. Art. 3 Nr. 1 Richtlinie (EU) 2016/680 auszugehen (Brockmann & Nugel, 2024, S. 664).

Als strafprozessuale Grundlage für den physischen Zugriff auf den EDR-Festspeicher kommen insbesondere die §§ 94, 98 und 110 StPO in Betracht, sei es durch Sicherstellung, Beschlagnahme oder Auslesung (BVerfGE 113, 29 Ls. 1; BVerfGK 1, 45, 47; Neuhaus et al., 2024, Rn. 200). Die Vorschriften der §§ 94 ff. StPO sind nach der Rechtsprechung des Bundesverfassungsgerichts trotz ihres Zuschnitts auf körperliche Gegenstände auch auf gespeicherte Daten anwendbar; sie entsprechen insofern dem Gebot der Normenklarheit, sodass keine grundsätzlichen verfassungsrechtlichen Bedenken gegen ihre Heranziehung bestehen (BVerfGE 113, 29, 50−52).

Gerade angesichts der geringen tatbestandlichen Anforderungen des § 94 Abs. 1 StPO bedarf es zur effektiven Sicherung der Grundrechtspositionen Betroffener einer einzelfallbezogenen Betrachtung der Verhältnismäßigkeit der Sicherungsmaßnahme unter Einbeziehung des jeweils beabsichtigten Verwendungszwecks (BVerfGE 20, 162, 286; 124, 58, 61), hier der Strafverfolgung. Zunächst ist festzuhalten, dass die Anfertigung einer Datenkopie unter Verhältnismäßigkeitserwägungen gegenüber einer Sicherstellung des Datenspeichers i. d. R. das Mittel der Wahl sein wird (Köhler, 2025, § 94 Rn. 18a). Angesichts des kurzen Zeitbereichs einer Speicherung von Daten um das Unfallereignis ergibt sich bei den persistenten EDR-Daten ein nur kurzer Datenausschnitt des bereits dargestellten Datenumfangs. Der Erkenntniswert dieser Informationen ist für eine (ergänzende) Unfallrekonstruktion sowie das vorausgehende Fahrverhalten allerdings hoch (mit konkreten Praxisbeispielen und zu-

gehörigen EDR-Daten Winkelmann, 2023, S. 5–6). Gerade bei schweren Verkehrsunfällen mit Personenschäden oder erheblichen Sachschäden wird eine Sicherung der EDR-Daten nur selten an Verhältnismäßigkeitserwägungen scheitern.

Doch auch bei leichten Verkehrsunfällen mit insbesondere nur geringen Sachschäden ist die Sicherung nicht pauschal mit Verweis auf die Verhältnismäßigkeit abzulehnen. In der zuletzt genannten Konstellation erscheint es sachgerecht, darauf abzustellen, ob der Verkehrsunfall in diesen Fällen nicht oder nur unter erheblichen Schwierigkeiten rechtssicher aufgeklärt werden kann – bei Bejahung wird unter weiterer einzelfallbezogener Würdigung des Falles regelmäßig eine Sicherung der EDR-Daten in Betracht kommen, die zugleich die Verhältnismäßigkeitsanforderungen wahrt. Insofern sollte die Sicherung von EDR-Daten in der Praxis als Standard der polizeilichen Unfallaufnahme bei Verkehrsunfällen mit Personenschaden und Straftatverdacht bei unklaren Beweisaussichten in Betracht gezogen werden. Hierfür könnte durch entsprechende Erlasslage der Innenministerien eine Prüfpflicht nebst der Benennung von Hilfsparametern geschaffen werden. Indes darf sie unter Verhältnismäßigkeitserwägungen nicht zur pauschalen Standardmaßnahme jeder Verkehrsunfallaufnahme erwachsen.

Für die Fahrzeugklassen M1 und N1 (Personenkraftwagen und leichte Nutzfahrzeuge) liegen nach Art. 4 Verordnung (EU) 2022/545 unionsweit harmonisierte Vorgaben zur Ausgestaltung der technischen Details des Datenabrufs vor. Dies erleichtert die Sicherung in der Praxis durch Standardisierung deutlich. Nach §§ 160 Abs. 1, 170 Abs. 1, 110 Abs. 1 und 3 S. 1 StPO obliegt die Durchsicht, auch von Daten auf Datenträgern (Köhler, 2025, § 110 Rn. 2a), grundsätzlich der Staatsanwaltschaft (Wenzel, 2016, S. 86). Nur nach Anordnung der Staatsanwaltschaft sind die Ermittlungspersonen (§ 152 GVG) hierzu befugt (§ 110 Abs. 1 StPO). Andernfalls besteht die Befugnis zur Durchsicht (hier der EDR-Daten) für Beamte nur bei Genehmigung durch den Inhaber. Da diese Daten im Zuge der europäischen Standardisierung heute aber zielgerichtet ausgelesen werden können, bleibt für eine klassische Durchsicht i. S. d. § 110 StPO nur wenig Raum. Vielmehr wird von einem zielgerichteten Zugriff zu sprechen sein. Am Ende der Sicherungsmaßnahme steht eine Sicherstellung nach § 94 Abs. 1 StPO oder eine Beschlagnahme nach Maßgabe der §§ 94 Abs. 2, 98 StPO.

Im Rahmen der Unfallermittlungen ist auch ein Zugriff auf fahrzeugbezogene (besser: fahrzeugbetreibungsbezogene) Datenbestände bei den Fahrzeugherstellern denkbar, weil immer mehr Automobilhersteller derartige Datensätze auf Backendservern speichern (Fothen et al., 2024, S. 201). Hierbei ist allerdings zu beachten, dass eine vollständige Übertragung der EDR-Daten „over-the-air“ nach der Verordnung (EU) 2019/2144 respektive (bei Eröffnung des Anwendungsbereichs) nach der Verordnung (EU) 2022/545 nicht vorgesehen ist. Jedoch ist die Übertragung einzelner Parameter nicht ausgeschlossen, sodass speziell bei (physischer) Unzugänglichkeit des EDR-Festspeichers (etwa nach einem Brand) der Zugriff auf Backendserverdaten bei den Fahrzeugherstellern ermittlungstechnisch relevant werden kann (Fothen et al., 2024, S. 202).

Daneben können sich aus den auf den Backendservern befindlichen Datensätzen im Einzelfall Ermittlungsansätze ergeben. Dass die Fahrzeughersteller etwa genaue Bewegungsdaten der Fahrzeuge speichern und in Datenbanken zusammenführen, zeigte eindrucksvoll die Presseberichterstattung zu Volkswagen-Fahrzeugen im Jahre 2024 auf, wonach eine Datenbank mit

Bewegungsdaten von 800.000 Elek-trofahrzeugen ungeschützt im Internet zugänglich war und in den Datensätzen auch Bewegungsdaten vorlagen, die u. a. Bezug zum Bundesnachrichtendienst aufwiesen (Der Spiegel, 2024). Die genauen Zugriffsvoraussetzungen sollen hier allerdings nicht weiter betrachtet werden, weil sich aufgrund der Vielfalt vernetzter Funktionen moderner Fahrzeuge in diesen Fällen mannigfaltige Abgrenzungsfragen zum Zugriff auf Kommunikationsdaten auch im Falle digitaler Dienste und bloßer Datenspeicherbestände (gespeicherte Daten auf Servern) stellen, für die in der StPO spezialgesetzliche Zugriffsbefugnisse normiert sind. Zu erwähnen sind hier insbesondere §§ 100a, 100j und 100k StPO.

Ferner ist zu berücksichtigen, dass ein zwangsweiser Zugriff bei international verteilter Server-Infrastruktur der Automobilhersteller regelmäßig zunächst die Feststellung des jeweiligen Serverstandorts voraussetzt, sofern eine Mitwirkung des Herstellers ausbleibt (Schlanstein, 2016, S. 205). Bei einem Standort außerhalb Deutschlands wird ein Zugriff häufig nur unter Nutzung der (Internationalen) Rechtshilfe möglich sein (Singelnstein, 2012, S. 597).

Anwenden (Apply)

Hiernach folgt die Datenauswertung. Dabei geht es um „die Identifikation und Auswertung von Datenbeständen. […Sie] ist daher [der] Kern und das Hauptanwendungsfeld IT-forensischer Ermittlungen“ (Marschall, 2019, S. 101). Die Staatsanwaltschaft kann sich bei der Auswertung der EDR-Daten neben den Ermittlungspersonen auch Sachverständiger oder sachverständiger Zeugen bedienen, §§ 161 Abs. 1 S. 1, 72 ff. StPO (Wenzel, 2016, S. 86–87).

Für die Auswertung und Interpretation der EDR-Daten ist die Hilfe technischer Sachverständiger zur Führung eines beweissicheren Verfahrens angezeigt (Winkelmann, 2023, S. 3). Dabei handelt es sich um Kfz-technische oder unfallanalytische Sachverständige (Schlanstein, 2016, S. 206). Die Staatsanwaltschaft kann den Sachverständigen eigenständig bestellen (§§ 161a Abs. 1 S. 2, 73 StPO), wobei nach dem staatsanwaltlichen Innenrecht gem. Nr. 70 Abs. 1 RiStBV vor Auswahl des Sachverständigen dem Verteidiger Gelegenheit zur Stellungnahme zu geben ist, soweit kein Eilfall oder ein wiederkehrender Standardfall ersichtlich ist (Krause, 2018, § 73 Rn. 26). Gem. § 162 StPO kann sie dies andernfalls bei dem Ermittlungsrichter beantragen (Güntge, 2025, § 73 Rn. 5).

Im Rahmen der Auswertung ist auch zu überprüfen, ob die Integrität der gesicherten EDR-Daten gegeben ist, die nach Art. 3 Verordnung (EU) 2022/545 gegen Manipulation zu schützen sind. Für die weitere Auswertung ist die Arbeit mit einer physikalischen Kopie und nicht mit dem Originaldatensatz entscheidend (Neuhaus et al., 2024, Rn. 210). Aus den gesicherten Datensätzen werden Erkenntnisse für die Bestimmung des Unfallhergangs gewonnen (Berechnungsbeispiele bei Winkelmann, 2023, S. 5–6). Dies erfolgt in einem wissenschaftlichen Vorgehen nach dem Stand der Technik (Morgenstern, 2011, S. 204).

Präsentieren (Present)

Die letzte Stufe der Forensik bildet die Interpretation. Gem. § 75 StPO ist der Sachverständige, auf den gem. § 72 StPO die Vorschriften über Zeugen entsprechend Anwendung finden, zur Erstattung eines Gutachtens verpflichtet (Wenzel, 2016, S. 87). Dies kann in Form eines Berichts oder Gutachtens erfolgen, der bzw. das Bestandteil der Ermittlungsakte wird und

im gerichtlichen Verfahren mündlich ausgeführt werden kann (Morgenstern, 2011, S. 204). Soweit hierbei personenbezogene Daten betroffen sind, bestimmt sich die weitere Datenverarbeitung nach §§ 483 ff. StPO. Diesbezüglich sind auch die dort normierten Anforderungen an die Zweckänderung zu beachten, die der Umsetzung der Grundsätze aus Art. 4 Abs. 1 lit. b und Abs. 2 Richtlinie (EU) 2016/680 dienen.

Die vorgenannten strafprozessualen Überlegungen lassen sich in Grundsätzen auch auf Ordnungswidrigkeitenverfahren übertragen, wenngleich dort insbesondere im Hinblick auf die Beweiserhebung erhöhte Anforderungen an die Verhältnismäßigkeit zu stellen sein werden (Fothen et al., 2020, S. 287), was im Einzelfall zu einer abweichenden Bewertung führen kann. Für Verkehrsunfallermittlungen dürfte eine polizeirechtliche Zielrichtung regelmäßig ausscheiden, doch sei bemerkt, dass auch im Bereich des (besonderen) Polizeirechts Fallkonstellationen vorstellbar sind, in denen eine Nutzung von EDR-Daten Relevanz entfalten könnte, etwa im Rahmen verwaltungsrechtlicher Ermittlungen seitens der Verkehrsbehörde. Indes dürfte in der Praxis nur selten das Bedürfnis nach einer eigenständigen verwaltungsrechtlichen Beweiserhebung bestehen, weil in derartigen Konstellationen parallel strafprozessuale oder ordnungswidrigkeitenrechtliche Ermittlungen laufen dürften und auf die dortigen Erkenntnisse gegebenenfalls unter Rückgriff auf nationale Akteneinsicht- und Zweckänderungsklauseln (BVerfGE 65, 1, 46; 141, 220, 324 Rn. 276) zugegriffen werden kann. Diesbezüglich ist allerdings die Beschränkung des Art. 6 Abs. 4 lit. d Verordnung (EU) 2019/2144 zu beachten.

Ausblick

Am Beginn nahezu jeder sachverständigen Unfallrekonstruktion steht die polizeiliche Spurensicherung an der Unfallstelle (Weber, 21. A. Rn. 1). Die Nutzung elektronischer Datenaufzeichnungen zur Rekonstruktion des Unfallgeschehens gehört zu den neueren Entwicklungen des Verkehrsunfallprozesses, wenn in Erinnerung gerufen wird, dass der Präsident des 28. Deutschen Verkehrsgerichtstages 1990 noch erfolglos die verpflichtende Einführung eines Unfalldatenschreibers forderte (vgl. Fothen et al., 2020, 284). Heute handelt es sich bei Neufahrzeugen um „Smart-Mobile“ (Weichert, 2016, 361), die ein breites Spektrum polizeilicher Erkenntnismöglichkeiten eröffnen.

Wegen seines besonders einfachen und rechtlich unaufwendigen Zugangs nimmt der Event Data Recorder (EDR) eine besondere Stellung zur Sicherung unfallrelevanter Daten ein. Während die klassischen Unfallspuren stets nur eine Momentaufnahme nach dem Ereignis liefern, dokumentiert der EDR die letzten Sekunden vor und während des Unfallgeschehens dynamisch. Dadurch können Konstellationen aufgeklärt werden, die früher oft im Bereich von Vermutungen und Wahrscheinlichkeitsannahmen verblieben. Eine Verwertung der Daten ist sowohl im Strafverfahren (vgl. etwa den sog. „Ku’damm-Raser“-Fall, LG Berlin, Urt. v. 27.02.2017, Az. 535 Ks 251 Js 52/16 (8/16)) als auch im Zivilprozess (vgl. OLG Hamm, Urt. v. 13.05.2019, Az. I-6 U 144/17) anerkannt.

Die aufgezeichneten Daten können dabei insbesondere zur Aufklärung des Unfallgeschehens sowie zur Erkennung möglicher Unfallmanipulationen beitragen (Freymann, 2025, Einl. Rn. 99 m. w. N.). In Fällen von Unfallflucht oder manipulierten Unfällen können EDR-Daten – bis-

weilen ganz ohne Sachverständigen – helfen, Widersprüche zwischen Behauptungen der Beteiligten und/oder dem Schadensbild aufzudecken. Die Bedeutung geht so weit, dass die Verweigerung der Auslesung eines Datenspeichers durch einen vom Versicherer beauftragten Sachverständigen gar zum Verlust von Ansprüchen aus einer Vollkaskoversicherung führen kann (LG Köln, Urt. v. 26.03.2020, Az. 24 O 236/19). Die Weigerung wurde als arglistige Verletzung der Aufklärungsobliegenheit des Versicherungsnehmers bewertet, die eine Leistungsfreiheit des Versicherers zur Folge hatte (OLG Köln, Beschl. v. 08.07.2020, Az. 9 U 111/20).

Perspektivisch besondere Bedeutung erlangt der EDR bei Delikten, die riskante oder rücksichtslos gesteigerte Fahrweisen unter Strafe stellen. Bei verbotenen Kraftfahrzeugrennen (§ 315d StGB) oder Gefährdungen des Straßenverkehrs (§ 315c StGB) lassen sich vielfach gerichtliche Feststellungen treffen, ob ein bewusstes Beschleunigen bzw. eine konstant hohe Geschwindigkeit vorlag oder ob es sich um eine kurzfristige Fehleinschätzung des Kfz-Führers handelte (Mehlich & Härter, 2026, S. 54). Damit verschiebt sich die Beweisgrundlage. Subjektive Einlassungen und vage Spurenbilder werden durch objektivierte Messdaten ergänzt. Behauptete Fehlreaktionen oder Wahrnehmungsdefizite, etwa die Einlassung eines „Augenblicksversagens“, werden überprüfbar.

Der Begriff des „Quantensprungs“ ist vor diesem Hintergrund nicht bloße Rhetorik, sondern beschreibt einen qualitativen Sprung in der Informationsdichte und -qualität. Die polizeiliche Unfallrekonstruktion wird sich zukünftig noch weiter von einem überwiegend induktiven, von Modellannahmen geprägten Verfahren zu einem stärker datenbasierten Prozess entwickeln, in dem Annahmen sich an digital dokumentierten Fahrverläufen messen lassen müssen. Dies eröffnet nicht nur neue Chancen für eine sachgerechte Aufklärung, sondern verändert auch die Dynamik der gerichtlichen Beweiswürdigung, in der digitale Fahrdaten zunehmend als zentrales Beweismittel in den Blick rücken.

Die Integration der EDR-Daten in die polizeiliche Arbeit ist hierbei nicht allein eine Frage der Technik, sondern erfordert organisatorische Anpassungen und rechtspolitische Weichenstellungen. Auf der operativen Ebene werden Antworten benötigt, wie EDR-Daten in standardisierte Unfallaufnahmeprozesse eingebettet werden können, ohne die Einsatzkräfte technisch zu überfordern oder die Einsatzzeiten insbesondere an der Unfallstelle unverhältnismäßig zu verlängern. Die bislang erprobten Pilotprojekte müssen nun „in die Fläche“ gebracht werden. Die digitale Unfallaufnahme via App kann hier ein weiterer wichtiger Baustein sein (vgl. MI NRW 2021).

Rechtspolitisch stellt sich die Frage, ob es bei der Anwendung der allgemeinen Vorschriften der Strafprozessordnung verbleiben kann oder spezifische Regelungen für datenintensive Fahrzeugtechnologien erforderlich sind. Bereits seit 2018 müssen Neufahrzeuge in Europa mit einem automatischen Notrufsystem (eCall) ausgestattet sein, das unter anderem die Koordinaten des Unfallorts übermittelt (Verordnung (EU) 2015/758). Zudem besteht bei hoch- und vollautomatisierten Kraftfahrzeugen nach § 63a StVG eine gesetzliche Pflicht zur Speicherung von GPS-Daten.

Wenngleich nach gegenwärtiger Rechtslage mit §§ 94 ff. StPO Eingriffsgrundlagen zur Verfügung stehen, insofern ein Zugriff in der polizeilichen Praxis rechtssicher möglich ist, wäre eine spezialgesetzliche Normierung begrüßenswert. Denkbar sind diesbezüglich sowohl

klarstellende Regelungen zur Datensicherung und -auswertung als auch verfahrensrechtliche Vorschriften, die Transparenz und Betroffenenrechte stärken. Denn nach Abschluss einer unfallfreien Fahrt entfällt regelmäßig das berechtigte Interesse an einer weiteren Speicherung dieser Daten (Weichert, 2016, 363).

Dies bildet die derzeitige einfachrechtliche Rechtslage allenfalls fragmentarisch und in unterschiedlichen Rechtsakten auf verschiedenen Normebenen (nationales Recht sowie Europäisches Unionsrecht) verstreut ab, was die polizeiliche Praxis vor die Herausforderung einer rechtssicheren Umsetzung stellt. Eine spezialgesetzliche und in sich geschlossene Regelungsstruktur, die das staatliche Interesse an Aufklärung und Datenspeicherung mit den Unions- und nationalen (Grundrechts-)Gewährleistungen EDR-spezifisch in einen Ausgleich bringt, würde perspektivisch dazu beitragen, dass die Verfolgungsbehörden EDR-Daten umfassender oder jedenfalls rechtssicherer zur Aufklärung heranziehen, weil insoweit eine rechtlich ausdifferenzierte Standardmaßnahme geschaffen würde. Vor dem Hintergrund, dass mit der zunehmenden Digitalisierung zusätzliche Datenquellen hinzutreten werden, erscheint eine zeitnahe rechtliche Einbettung des EDR in ein umfassenderes „Fahrzeugdatenrecht“ sinnvoll.

Referenzen

Appel, H., Krabbel, G., & Vetter, D. (2002). Unfallforschung, Unfallmechanik und Unfallrekonstruktion. 2. Auflage. Vieweg & Teubner. https://doi.org/10.1007/978-3-322-83030-2

Berg, A. (2025). Schutz von Insassen und Kontrahenten bei Pkw-Unfällen: Historische Entwicklungen und aktueller Stand von Systemen der passiven und integralen Sicherheit. Springer Vieweg. https://doi.org/10.1007/978-3-662-71655-7

Brockmann, O., & Nugel, M. (2024). Unfallrekonstruktion mithilfe eines Ereignisspeichers im Jahr 2024 – eine interdisziplinäre Betrachtung, DAR, 12, 661–667.

Burmann, M., & Schmedding, K. (2015). Unfallrekonstruktion im Verkehrsprozess: Sachverständige – Gutachten – Fehlerquelle, 2. Auflage, Deutscher Anwaltverlag.

Burg, H., & Moser, A. (2017). Handbuch Verkehrsunfallrekonstruktion: Unfallaufnahme, Fahrdynamik, Simulation. 3. Auflage. Springer Vieweg. https://doi.org/10.1007/978-3-658-16143-9

Cinar, T. J. (2025). Privates Datenschutzrecht im Lichte der Grundrechte: Eine Untersuchung am Beispiel der Verarbeitung von Kraftfahrzeugdaten. Materialien zur rechtswissenschaftlichen Medien- und Informationsforschung: Band 86. Nomos. https://doi.org/10.5771/9783748968214

Der Spiegel (2024). Datenleck beim Volkswagen-Konzern: Wir wissen, wo dein Auto steht. Beuth, P., Flüpke, Hoppenstedt Heinrichs, M., Kreil, M., Rosenbach, M., & Wilkin, R. Der Spiegel 1/2025. 27.12.2024. https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027

Der Tagesspiegel (2010). Brandenburg Bagatellunfälle: Land prüft Blaulichtsteuer. Keine Gratis-Hilfe der Polizei bei Kleinunfällen? 16.10.2010. https://www.tagesspiegel.de/potsdam/brandenburg/bagatellunfalleland-pruft-blaulichtsteuer-keine-gratis-hilfe-der-polizei-bei-kleinunfallen-7554388.html

Die Zeit (2025). Projekt Digitale Unfallspuren. Polizei liest Unfalldaten aus – Ministerin will Ausbau. 5.8.2025. https://www.zeit.de/news/2025-08/05/polizei-liest-unfalldaten-aus-ministerin-will-ausbau

Dürnberger, S., & Kreutner, M. (2017). EDR-Daten heute und in Zukunft, VKU, 10, 328–341.

Eisenberg, U. (2017). Beweisrecht der StPO: Spezialkommentar. 10. Auflage. C.H. Beck.

Fothen, C., Böhm, K., & Paula, D. (2020). Kann die Verwendung digitaler Fahrzeugdaten zur Rekonstruktion von Verkehrsunfällen unterhalb der Schwelle schwerster Unfallereignisse verhältnismäßig sein? NZV, 6, 284–289.

Fothen, C., Feuerer, A., & Böhm, K. (2024). Die Anforderung von Backendserverdaten für die Aufklärung von Verkehrsunfällen. NZV, 5, 201–206.

Fothen, C., & Böhm, K. (2026). Mehr Verkehrssicherheit durch aussagekräftigere Unfalldaten: Zum Arbeitskreis VII des 64. Deutschen Verkehrsgerichtstags. NZV, 1, 45–48.

Freymann, H.-P. (2025). juris Praxiskommentar. Straßenverkehrsrecht. In H.-P. Freymann, W. Wellner, & M. Trésoret (Hrsg.). 3. Auflage. Juris.

Grüneberg, C. (2023). 4. Haftungsvoraussetzungen und Haftungsverteilung. In M. Burmann & R. Heß (Hrsg.), Handbuch des Straßenverkehrsrechts. Rechtsstand: August 2023, 48. Ergänzungslieferung. C.H. Beck.

Güntge, G. F. (2025). StPO § 73. In T. Rotsch, F. Saliger & M. Tsambikakis (Hrsg.), Strafprozessordnung Kommentar. Nomos.

Hamann, H. (2025). § 22 Die außergerichtliche Geltendmachung von Haftpflichtansprüchen gegen Schädiger und Haftpflichtversicherung – Schadenmanagement. In B. M. Höke (Hrsg.), Münchener Anwaltshandbuch. Straßenverkehrsrecht. 6. Auflage. C.H. Beck.

Jahn, M., & Brodowski, D. (2020). Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision. In E. Hoven & H. Kudlich (Hrsg.), Digitalisierung und Strafverfahren (S. 67–102). Nomos. https://doi.org/10.5771/9783748908708-67

Köhler, M. (2025). StPO § 94. StPO § 110. In B. Schmitt & M. Köhler, Kommentar Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 68. Auflage. C.H. Beck.

König, P. (2023). 13. Straf- und Ordnungswidrigkeitenrecht. In M. Burmann & R. Heß (Hrsg.), Handbuch des Straßenverkehrsrechts. Rechtsstand: August 2023, 48. Ergänzungslieferung. C.H. Beck.

Krause, D. M. (2018). StPO § 73. In Löwe-Rosenberg. Die Strafprozeßordnung und das Gerichtsverfassungsgesetz: Großkommentar. J.-P. Becker, V. Erb, R. Esser, K. Graalmann-Scheerer, H. Hilger, A. Ignor (Hrsg.), Zweiter Band (§§ 48–93), 27. Auflage. de Gruyter.

Kreutner, M. & Nugel, M. (2023). Auslesen von Daten aus dem EU-Ereignisspeicher von Fahrzeugen zur Unfallrekonstruktion, NJW, 4, 177–183.

Kühne, A. (2022). Rechtshandbuch Connected Cars. In A. Kühne & R. Nack (Hrsg.). C.H. Beck.

Marschall, K. (2019). Rechtsverträgliche Gestaltung IT-forensischer Systeme: Eine Untersuchung am Beispiel der Aufdeckung und Beweisbarkeit von Versicherungsbetrug. DuD-Fachbeiträge. Springer Vieweg. https://doi.org/10.1007/978-3-658-26237-2

Mehlich, A., & Härter, J. (2025). Automotive IT (AIT) als „Fundgrube“ polizeilicher Arbeit. In W. Honekamp & M. Klingelhöfer (Hrsg.), Polizei-Informatik 2025, Band 27. 213–222. Verlag für Polizeiwissenschaften.

Mehlich, A., & Härter, J. (2026). Das vernetzte Fahrzeug als mobiles Datendepot. Einsatz des Event Data Recorders (EDR) zur Sicherung digitaler Fahrzeugdaten in der Car-Forensik. In M. Höhner, T. Huschbeck & M. Sondermann (Hrsg.), Verkehrssicherheit im Wandel: Prävention, Diversion und digitale Ermittlungsansätze. 35–58. Verlag für Polizeiwissenschaften.

Melchers, W. (1994). Polizeiliche und private Verkehrsunfallaufnahme. NZV, 1, 1–5.

Mildner, R., Ziller, T., & Baiocchi, F. (2024). Car IT kompakt Reloaded: Das Auto der Zukunft – Vernetzt und autonom fahren. Springer Vieweg. https://doi.org/10.1007/978-3-658-44319-1

Ministerium des Innern des Landes Nordrhein-Westfalen (2021). Pressemitteilung vom 09.04.2021. Kein Papier mehr: NRW-Polizei erfasst Unfälle digital. https://polizei.nrw/presse/kein-papier-mehr-nrw-polizei-erfasst-unfaelle-digital

Ministerium des Inneren, für Digitalisierung und Kommunen des Bundeslandes Baden-Württemberg (2021). Pressemitteilung vom 26.05.2021. Digitale Spurensicherung und Spurenauswertung.https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/digitale-spurensicherung-und-spurenauswertung

Morgenstern, H. (2011). Zuverlässigkeit von IP-Adressen-Ermittlungssoftware: Zur Sicherheit der eingesetzten Programme und Verfahren zur Verletzungsdokumentation. CR, 3, 203–208. https://doi.org/10.9785/ovs-cr-2011-203

Neuhaus, R., Artkämper, H., & Weise, G. (2024). Kriminaltechnik und Beweisführung im Strafverfahren. 2. Auflage. NJW Praxis: Band 96. C.H. Beck.

Paul, S., & de Valck, M. (2023). Sicherung digitaler Fahrzeugspuren zur Verkehrsunfallaufnahme. In Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis. D. Wehe & H. Siller (Hrsg.). 2. Auflage, 1585–1600. Springer Gabler. https://doi.org/10.1007/978-3-658-34388-0_92

Raab-Düsterhöft, A. (2024). IT-Forensik. Ein Grundkurs. Springer Vieweg. https://doi.org/10.1007/978-3-662-69090-1

Reid, M. (2024). 2.8.2 Your Privacy on the Road: What is Collected and How it is Utilized. In B. H. Oppermann & P. Buck-Heeb (Hrsg.), Autonomes Fahren: Rechtshandbuch. 3. Auflage. C.H. Beck.

Reif, K. (2016). Sensoren im Kraftfahrzeug. 3. Auflage. Bosch Fachinformation Automobil. Springer Vieweg. https://doi.org/10.1007/978-3-658-11211-0

Schlanstein, P. (2016). Nutzung von Fahrzeugdaten zur Optimierung der Verkehrsunfallaufnahme. NZV, 5, 201–209.

Schmid, A., & Wessels, F. (2017). Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG. NZV, 8, 357–364.

v. Schönfeld, M. (2015). Ein fahrbarer Datensatz: Datenschutzrechtliche Probleme im modernen Auto, DAR, 11, 617–622.

Seckelmann, M. (2024). 2.7.1 Elektromobilität in der Smart City: Smarte Mobilität und digitale Vernetzung als Mittel zur Unterstützung der Energiewende. In B. H. Oppermann & P. Buck-Heeb (Hrsg.), Autonomes Fahren: Rechtshandbuch. 3. Auflage, C.H. Beck.

Singelnstein, T. (2012). Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co. NStZ, 11, 593–606.

Statistisches Bundesamt (2025). Hauptverursacher von Unfällen mit Personenschaden. 16.7.2025. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/Tabellen/hauptverursacher-fahrzeugart.html

Tinnefeld, R. (2025). Datenschutz im Internet. Rechtshandbuch. In R. Schwartmann, K. Benedikt & Y. Reif (Hrsg.). C.H. Beck.

Transformationswissen BW (2021). Automotive in Bewegung. Landesagentur für neue Mobilitätslösungen und Automotive Baden-Württemberg et al. (Hrsg.). https://www.transformationswissen-bw.de/fileadmin/media/Publikationen/e-mobil_Studien/Wissen_kompakt_Fahrzeugdaten.pdf

Weber, M. (2023). 21. Unfallrekonstruktion. In M. Burmann & R. Heß (Hrsg.), Handbuch des Straßenverkehrsrechts. Rechtsstand: August 2023, 48. Ergänzungslieferung. C.H. Beck.

Weichert, T. (2016). Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung, SVR, 10, 361–367.

Wenzel, H. (2016). Rechtliche Grundlagen der IT-Forensik. NZWiSt, 3, 85–93.

Wiebe, A., Helmschrot, C., & Kreutz, O. (2023). Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft. Schlussbericht., Referat 121 Digitalisierung und Vernetzung; Internetplattformen. https://data.bundesnetzagentur.de/Bundesnetzagentur/DE/Fachthemen/Digitalisierung/Daten/Datenoekonomie/schlussbericht.pdf

Winkelmann, A. (2023). „Einzelraser“ nach § 315d Abs. 1 Nr. 3 StGB und der Nachweis durch digitale Fahrzeugdaten. DAR, 1, 2–7.

Vom Datenträger zur Cloud – Die Entwicklung der digitalen Forensik in der Polizeiarbeit

Heiko Rittelmeier

Die Digitalisierung macht heute vor keinem Lebensbereich mehr Halt und hat auch die Kriminalistik fundamental verändert. Während früher ausschließlich physische Spuren – beispielsweise Fingerabdrücke, serologische Spuren, Schuhsohlenabdrücke – am Tatort gesichert wurden, spielen digitale Beweismittel heute in nahezu jedem Ermittlungsverfahren eine mehr oder weniger zentrale Rolle, unabhängig vom konkreten Delikt (Bundeskriminalamt [BKA], n.d.-a). Alle möglichen Arten von Daten, elektronische Dokumente, E-Mails, Chat-Protokolle, Standortdaten von Mobiltelefonen, Netzwerkprotokolle oder sonstige technische Aufzeichnungen sind in der heutigen Polizeiarbeit unverzichtbare Informationsquellen geworden, die die klassischen materiellen Spuren mindestens ergänzen oder teilweise sogar ersetzen und die in vielen Fällen zur Fallaufklärung unerlässlich sind.

Die digitale Forensik ist die wissenschaftliche Disziplin, die sich mit der gerichtsverwertbaren Identifikation, Sicherung, Analyse und Präsentation digitaler Beweismittel befasst (Palmer, 2001). Streng genommen ist sie Teilgebiet der Kriminaltechnik, real verbindet sie Informatik mit Strafrecht und Strafprozessrecht, wie es beispielsweise die medizinische Forensik in ihrem Spezialbereich tut. Eine Besonderheit der digitalen Forensik liegt dabei in der Fragilität und Volatilität der Beweismittel: Digitale Daten können leicht verändert oder gelöscht werden, was strenge methodische Anforderungen an die Arbeit der Forensiker stellt – mehr noch: Veränderung ist sozusagen Kern der Existenz digitaler Daten.

Die Entwicklung dieser wissenschaftlichen Disziplin in Deutschland und Europa verlief dabei nicht linear und nicht als Selbstzweck, sondern wurde aufgrund des vorliegenden Bedarfs durch technologische Innovationen und organisatorische Reformen innerhalb der Polizeibehörden sowie durch den wachsenden internationalen Austausch geprägt. Der vorliegende Text zeichnet diesen Weg nach, beginnend mit den Pionierjahren der 1990er Jahre über die Phase der Professionalisierung und Standardisierung um die Jahrtausendwende bis hin zu den aktuellen Herausforderungen durch Cloud-Computing, das Internet der Dinge (IoT) und Künstliche Intelligenz (KI).

Begriffsdefinition und methodische Grundlagen

Bevor die historische Entwicklung nachgezeichnet werden kann, müssen die grundlegenden Begriffe und methodischen Prinzipien der digitalen Forensik definiert werden. Diese bilden das Fundament für alle nachfolgenden Abschnitte und erklären, warum bestimmte Standards in der Praxis unverzichtbar sind.

Der Begriff „digitale Forensik“ wurde erst in den späten 1990er Jahren definiert; zuvor war in der Fachliteratur und Praxis überwiegend von „Computerforensik“ oder auch „IT-Forensik“ die Rede (Open University, n.d.). Während in den ersten Jahren der Begriff „Computerforensik“ wahrscheinlich alle relevanten Bereiche abdeckte, wurde im Laufe der Zeit durch die zunehmend breiter werdenden Themen eine weitere Fassung des Begriffs erforderlich,

eben die „digitale Forensik“. Der erste Digital Forensic Research Workshop (DFRWS) im Jahr 2001 definierte die Disziplin als „die Verwendung wissenschaftlich abgeleiteter und bewährter Methoden zur Konservierung, Sammlung, Validierung, Identifizierung, Analyse, Interpretation, Dokumentation und Präsentation digitaler Beweise, die aus digitalen Quellen zum Zweck der Erleichterung oder Weiterentwicklung der Rekonstruktion von Ereignissen als kriminell eingestufter Handlungen stammen“ (Palmer, 2001, S. 16). In Deutschland hat sich analog zu anderen forensischen Disziplinen zudem der Begriff der „forensischen Informatik“ als akademische Disziplin etabliert, die die theoretischen Grundlagen der digitalen Beweissicherung systematisch erforscht (Dewald, 2015).

Der typische, standardisierte forensische Untersuchungsablauf gliedert sich nach gängiger Definition in mehrere Phasen: Identifikation potenzieller Beweisträger, Sicherung und Akquise der Daten – idealerweise durch ein bitgenaues forensisches Abbild (Image) des Originaldatenträgers –, anschließende Analyse und schließlich die gerichtsfeste Dokumentation und Präsentation der Ergebnisse (National Institute of Standards and Technology [NIST], 2014). Auch wenn es mittlerweile weitere definierte Workflows gibt, die teilweise verfeinerte Schritte umfassen, gilt die genannte Definition im Kern bis heute. Ein fundamentales Prinzip lautet dabei, dass keine Untersuchungshandlung die Originaldaten verändern darf (auch wenn das in vielen Anwendungsfällen heute nicht mehr garantiert werden kann). Die Integrität der Beweismittel muss durch kryptografische Hashwerte (z. B. MD5, SHA-256) nachgewiesen bzw. überhaupt erst prüfbar gemacht werden. Ein Hashwert lässt sich als digitaler Fingerabdruck beschreiben: Ein Algorithmus erzeugt aus dem Inhalt einer Datei eine eindeutige Zeichenfolge, die sich bereits bei der Veränderung eines einzelnen Bits komplett verändert – sodass Manipulationen ausgeschlossen oder zumindest erkannt werden können. Dieses Prinzip findet sich in der britischen ACPO-Richtlinie von 1998 ebenso wie in der späteren ISO/IEC 27037:2012 (Association of Chief Police Officers [ACPO], 1998; International Organization for Standardization [ISO/IEC], 2012).

Das Konzept der Chain of Custody – der lückenlosen Dokumentation aller Personen und Handlungen, die Zugang zu einem Beweismittel hatten – ist ebenfalls ein wesentlicher Aspekt der digitalen Forensik. Der Nachweis einer lückenlosen Beweiskette ist die Grundlage dafür, dass digitale Spuren vor Gericht standhalten können. Fehlende oder unterbrochene Chain-of-Custody-Dokumentationen können im Extremfall zur Unverwertbarkeit von Beweisen führen – mit potenziell gravierenden Folgen für die Strafverfolgung.

Vorläufer und Pionierphase (1980er Jahre)

Die Anfänge der digitalen Forensik liegen in einer Zeit, in der Computer noch eine Randerscheinung in der Polizeiarbeit darstellten. Dennoch wurden in den 1980er Jahren die ersten institutionellen Strukturen geschaffen, die den Weg für die spätere Professionalisierung ebneten.

Die digitale Forensik entstand schon deutlich vor dem Internet in einer Zeit, in der persönliche Computer („Personal Computer – PC“) eine wachsende Verbreitung erlebten. Als eine der ersten Behörden weltweit erkannte das Federal Bureau of Investigation (FBI) in den Vereinigten Staaten die Notwendigkeit spezialisierter Organisationseinheiten für die Untersuchung von Computern im Rahmen von Ermittlungen. Diese Erkenntnis wurde zum Anlass

genommen, um 1984 das FBI Computer Analysis and Response Team (CART) zu gründen. Rückblickend wurde damit wohl der Grundstein für die institutionelle Computerforensik gelegt (Open University, n.d.). Schon zu diesem Zeitpunkt bestand die Einheit im Übrigen aus Polizeibeamten und zivilen Fachleuten – ein Modell, das sich bis heute in den meisten derartigen Organisationseinheiten gehalten hat.

In Europa waren es zunächst die britischen Behörden, die ähnliche Schritte unternahmen. 1985 richtete die Londoner Metropolitan Police im Rahmen der Fraud Squad eine spezialisierte Einheit für Computerkriminalität unter der Leitung von John Austen ein (Open University, n.d.). Diese frühen Einheiten arbeiteten noch weitgehend ohne standardisierte Methoden oder Verfahrensanweisungen, da derartige Dokumente zu diesem Zeitpunkt schlicht noch nicht verfügbar waren. Die ersten „Computerforensiker" waren typischerweise Strafverfolgungsbeamte, die privat Computerkenntnisse erworben oder ein grundlegendes Interesse an der Technik hatten und dieses nun in ihren täglichen Dienst einbrachten (Open University, n.d.). Nicht selten geschah dies mangels strukturierter Aus- und Weiterbildungsangebote auf Basis von Versuch und Irrtum.

In Deutschland verlief die Entwicklung zunächst langsamer. Zwar war eine starke Kriminaltechnikabteilung seit der Gründung des Bundeskriminalamts (BKA) im Jahr 1951 stets ein wichtiger Bestandteil der Behörde, deren Schwerpunkte lagen jedoch im Bereich der klassischen naturwissenschaftlich-forensischen Methoden – Schusswaffen, Serologie, Toxikologie, Daktyloskopie und Schriftgutachten (BKA, n.d.-b). Ab Mitte der 1960er Jahre wurde im BKA die elektronische Datenverarbeitung eingeführt, sie diente zu dieser Zeit jedoch primär der Verwaltung polizeilicher Daten, wie dem 1972 beschlossenen INPOL-System, und war noch sehr weit entfernt von einer forensischen Spurensicherung an digitalen Tatorten (Cilip, 2020).

Die westdeutsche Polizeilandschaft der 1980er Jahre war von der Auseinandersetzung mit dem RAF-Terrorismus und dem Bemühen, die Möglichkeiten der elektronischen Datenverarbeitung für die Verbrechensbekämpfung nutzbar zu machen, geprägt. Gleichzeitig waren aber noch eher Fernschreiber und Schreibmaschine in den polizeilichen Amtsstuben state of the art. Kenneth S. Rosenblatt, US-amerikanischer Jurist und früher Experte für Computerkriminalität, beschrieb 1995 die Ausgangslage in dieser Zeit recht treffend so: „Die Beschlagnahme, Aufbewahrung und Analyse von auf einem Computer gespeicherten Beweisen ist die größte forensische Herausforderung für die Strafverfolgungsbehörden in den 1990er Jahren" (zitiert nach Open University, n.d.).

Die 1990er Jahre: Institutionalisierung und erste Standards

Die 1990er Jahre markierten den entscheidenden Wendepunkt von der informellen Praxis zur systematischen Professionalisierung. In Deutschland setzte sich die digitale Kriminaltechnik langsam durch, während auf europäischer Ebene erste Standards entwickelt wurden, die bis heute Gültigkeit besitzen.

Digitale Kriminaltechnik beim BKA und in den Ländern

In den 1990er Jahren setzte in Deutschland langsam der Wandel ein. Bei den meisten Landespolizeien wurden vernetzte Computer flächendeckend eingeführt, vor allem ab der zweiten Hälfte des Jahrzehnts teilweise erstmalig auf Basis von verbreiteten Microsoft-Systemen (üblich waren davor oft UNIX-basierte Terminalsysteme). Damit ging auch die systematische Auseinandersetzung mit digitalen Beweismitteln einher (Polizeigeschichte NRW, 2023). Zwei Entwicklungen der frühen 1990er Jahre spielten dabei eine wichtige Rolle: die Einführung des Automatisierten Fingerabdruck-Identifizierungssystems (AFIS) im Jahr 1993 beim BKA sowie die Einrichtung der zentralen DNA-Analysedatei im Jahr 1998.

AFIS war ein Quantensprung für die biometrische Identifizierung: Statt einer bis zu 90 Minuten dauernden Arbeit von Daktyloskopen, um die Minutien eines Fingerabdrucks manuell zu erfassen, dauerte der Prozess nun nur noch rund drei Minuten (BKA, n.d.-c). Im Kern basierte das System auf der mathematischen Codierung anatomischer Merkmale und ermöglichte erstmals den automatisierten Abgleich von Tatortspuren mit dem Bestand – auch bei unvollständigen Abdrücken (BKA, n.d.-c). Im Jahr 2003 wurde EURODAC, ein auf AFIS basierendes europaweites Fingerabdruckidentifizierungssystem, in Betrieb genommen.

1998 wurde die DNA-Analysedatei beim BKA eingerichtet und erlaubte erstmals den bundesweiten automatisierten Abgleich genetischer Profile (BKA, n.d.-b). Bei beiden Systemen – AFIS und DNA-Datei – handelt es sich zwar im engeren Sinne nicht um Werkzeuge der digitalen Forensik, sie veranschaulichen jedoch die zunehmende Digitalisierung der Kriminaltechnik und das wachsende Vertrauen der Ermittlungsbehörden in computergestützte Analyseverfahren. Die Erfahrungen mit diesen Systemen waren sehr wahrscheinlich auch ein Treiber für die Digitalisierung in anderen Bereichen.

In den Landeskriminalämtern der Bundesländer – teilweise auch schon bei den kriminalpolizeilichen Dienststellen der Landespolizeien – wurden zeitgleich erste spezialisierte Arbeitsgruppen eingerichtet, die sich mit der Auswertung von Computern und Datenträgern im Rahmen von Ermittlungsverfahren befassten. Die Delikte wurden zu dieser Zeit als „IuK-Kriminalität“ beschrieben, wobei die Abkürzung für „Information und Kommunikation“ steht. Der heute übliche Begriff „Cybercrime“ existierte zu diesem Zeitpunkt noch nicht. Die Spezialdienststellen hießen damals auch noch nicht „digitale Forensik“, sondern hatten andere Namen wie „RBA“ in Bayern oder „RBE“ in Thüringen („RBA“ – **R**egionale **B**eweissicherungs- und **A**uswertestelle, „RBE“ – **R**egionale **B**eweissicherungs**E**inheit). Die Arbeit der dortigen Mitarbeiter war für eine relativ lange Zeit uneinheitlich und nicht standardisiert – geprägt von den individuellen Kenntnissen und Erfahrungen einzelner Beamter in Ermangelung übergreifender Ausbildungs- und Qualitätsstandards. In vielen Ländern wurden die Organisationseinheiten später in „digitale Forensik“ umbenannt, wenn auch teilweise relativ spät (z. B. in Bayern im Zuge einer Umstrukturierung im Jahr 2021), in einigen Bereichen werden die alten Bezeichnungen zum Zeitpunkt der Erstellung dieses Artikels immer noch genutzt (z. B. in Thüringen).

Rechtliche Grundlagen in Deutschland

Ein wesentliches rechtliches Problem der digitalen Forensik bestand zur damaligen Zeit darin, dass die bestehenden Strafprozessordnungen der meisten Länder nicht auf digitale Beweismittel ausgelegt waren. Die Schöpfer der Gesetze hatten keine Vorstellung davon, dass Beweismittel auch „nicht-stofflich" vorliegen könnten. Die deutsche Strafprozessordnung (StPO) regelt in den §§ 94 ff. die Sicherstellung und Beschlagnahme von Beweismitteln. Diese Vorschriften gelten seit Inkrafttreten der StPO im Jahr 1879 inhaltlich nahezu unverändert und sehen Datenträger als Gegenstand der Sicherstellung und Beschlagnahme nicht explizit vor (Bundesverfassungsgericht [BVerfG], 2005).

In der Rechtspraxis behalf man sich damit, den Datenträger – also die physische Festplatte – als Beweisgegenstand gemäß § 94 StPO zu behandeln. Das Bundesverfassungsgericht (BVerfG) klärte grundlegende verfassungsrechtliche Fragen in seinem Beschluss vom 12. April 2005 (Az. 2 BvR 1027/02). Es stellte fest, dass die StPO die Sicherstellung und Beschlagnahme von Datenträgern und den darauf gespeicherten Daten als Beweisgegenstände erlaubt, dass aber bei Durchsuchungen der Zugriff auf für das Verfahren bedeutungslose Informationen im Rahmen des Vertretbaren vermieden werden muss (BVerfG, 2005). Damit wurde auch ohne explizite Regelung in der StPO ein rechtssicherer Handlungsrahmen geschaffen.

Die Frage der Verwertbarkeit digitaler Beweismittel blieb in Deutschland – und ebenso in anderen europäischen Ländern – lange Zeit rechtlich ungeklärt und wurde weitgehend durch richterliche Entscheidungen geprägt (Peter Lang Verlag, 2019). Diese Rechtsunsicherheit wurde bedingt durch das Fehlen einschlägiger Normen und trieb die Notwendigkeit der Standardisierung forensischer Methoden voran, da nur bei Anwendung anerkannter Verfahren die Integrität der Beweise glaubhaft gemacht werden konnte. Nicht zuletzt tat sich auch die Justiz in der Praxis schwer mit diesem neuen Typus von Beweismitteln.

Europäische Vernetzung: Die Gründung von ENFSI

Parallel zur nationalen Entwicklung begann in Europa die institutionelle Vernetzung forensischer Wissenschaftsinstitute. Die Idee zur Gründung eines europäischen Netzwerks forensischer Laboratorien entstand zu Beginn der 1990er Jahre auf Initiative von Direktoren staatlicher forensischer Institute in Westeuropa (Kopp & Sprangers, 2002). Auf einer Vorbereitungssitzung im Jahr 1993 in Rijswijk (Niederlande), an der Vertreter aus elf westeuropäischen Laboratorien teilnahmen, wurde der Grundstein zum ENFSI gelegt (European Network of Forensic Science Institutes [ENFSI], 2020).

Am 20. Oktober 1995 fand die offizielle Gründungsversammlung des European Network of Forensic Science Institutes (ENFSI) in Rijswijk statt. 25 Gründungsmitglieder aus 17 europäischen Ländern unterzeichneten ein Memorandum of Understanding, das die Grundsätze und die Arbeitsweise der Organisation festlegte (ENFSI, 2020). Ziel war es, den fachlichen Dialog unter europäischen forensischen Wissenschaftlern zu fördern, die Qualität forensischer Dienstleistungen zu verbessern und gemeinsame Standards zu entwickeln.

Schon relativ kurz darauf, im Jahr 1998, wurde in Prag die Forensic Information Technology (FIT) Working Group des ENFSI gegründet – als erste spezialisierte europäische Arbeitsgruppe, die sich ausschließlich der digitalen Forensik widmete (ENFSI, 2020). Damit wird deutlich, wie früh die Bedeutung der Informationstechnologie als eigene forensische Disziplin erkannt wurde. Die FIT-Arbeitsgruppe veröffentlichte in den Folgejahren Praxisleitlinien und Best-Practice-Empfehlungen für die forensische IT-Untersuchung. Auch wenn die ENFSI-Leitlinien keine rechtlich bindende Wirkung entfalten, haben sie dennoch eine hohe praktische Relevanz: Sie definieren den wissenschaftlichen Qualitätsstandard, der von allen seriösen Wissenschaftlern und Instituten einzuhalten ist. Es handelt sich im Kern um die Regeln der guten Laborarbeit in digitalforensischen Labors, von denen nur in begründeten Fällen abgewichen werden darf, wenn man die erzielten Ergebnisse nicht infrage stellen will.

Britische Pionierarbeit: Die ACPO-Leitlinien von 1998

In Großbritannien nahm die Professionalisierung der digitalen Forensik besonders früh und sehr systematisch Fahrt auf. In den Jahren 1994 und 1995 fanden am Police Staff College in Bramshill richtungsweisende Konferenzen statt, die auf Initiative des Serious Fraud Office und des Inland Revenue zusammengerufen wurden und an denen Ermittler und technische Spezialisten der britischen Strafverfolgungsbehörden teilnahmen (Open University, n.d.). Aus diesen Treffen entstand die moderne britische Methodik der digitalen Forensik. „Inland Revenue“ war zu diesem Zeitpunkt der Name der Steuerbehörde des Vereinigten Königreichs, später wurde diese im Rahmen einer Fusion mit „HM Customs and Excise“ abgelöst vom „HM Revenue & Customs“ (HMRC) (ca. 2005).

Im Jahr 1998 veröffentlichte die Association of Chief Police Officers (ACPO) erstmals ihren Good Practice Guide for Digital Evidence – ein Leitfaden, der vier grundlegende Prinzipien für die Handhabung digitaler Beweismittel definierte (ACPO, 1998). Diese Prinzipien lauten sinngemäß:

1. Keine Handlung darf Daten verändern, die später als Beweismittel dienen könnten.
2. Wer es dennoch für notwendig hält, auf Originaldaten zuzugreifen, muss dafür qualifiziert sein und seine Handlungen gerichtsfest begründen können.
3. Ein Protokoll aller auf digitale Beweismittel angewandten Maßnahmen muss erstellt und aufbewahrt werden.
4. Der verantwortliche Ermittler ist dafür zuständig, dass geltende Gesetze und diese Prinzipien eingehalten werden (ACPO, 1998).

Diese vier ACPO-Prinzipien haben sich nicht nur im Gebiet des Vereinigten Königreichs ausgewirkt, sie haben die Praxis der digitalen Forensik weit über die britischen Grenzen hinaus geprägt und wirkten auch in Deutschland und anderen europäischen Staaten normbildend. Im Kern entsprechen diese heute noch dem allgemein akzeptierten Standard.

Jahrtausendwende und Professionalisierung (1999–2007)

Mit dem Übergang ins neue Jahrtausend beschleunigte sich die Entwicklung. Professionelle Softwarelösungen kamen auf, wissenschaftliche Netzwerke etablierten sich, und neue Teildisziplinen wie die Forensik mobiler Endgeräte (Telefone, Smartphones) entstanden.

Die Entwicklung forensischer Softwarewerkzeuge

Um die Jahrtausendwende herum verursachte die aufstrebende digitale Forensik einen technologischen Entwicklungsschub, der ihre Möglichkeiten erheblich erweiterte. Im Jahr 1997 gründete Shawn McCreight das Unternehmen Guidance Software in Pasadena, Kalifornien, mit dem expliziten Ziel, Strafverfolgungsbehörden bei der sicheren Suche auf digitalen Medien zu unterstützen (Guidance Software, 2012). Das Ergebnis war das Programm „Expert Witness“, das erste professionelle forensische Tool, das Windows-basiert arbeitete und 1998 erstmals veröffentlicht wurde. Im selben Jahr wurde die Software zu „EnCase“ umbenannt. Der von EnCase entwickelte Standard zur Speicherung von Datenträgersicherungen („Expert Witness Format – EWF“) wird heute noch von den meisten Forensikern genutzt.

EnCase ermöglichte erstmals eine benutzerfreundliche, grafisch gestützte Untersuchung von Datenträgern auf der Basis forensisch gesicherter Bit-für-Bit-Kopien (Images). Das Tool konnte gelöschte Dateien wiederherstellen, versteckte Daten sichtbar machen und einen vollständigen Prüfpfad aller Untersuchungsschritte generieren. Bis zur Mitte der 2000er Jahre entwickelte es sich zum De-facto-Standard in der Strafverfolgung weltweit, nicht nur in Deutschland und Europa. Im Jahr 2002 wurde EnCase Enterprise eingeführt, das erste netzwerkfähige forensische Tool, das eine Fernuntersuchung von Systemen über Netzwerkverbindungen ermöglichte.

Parallel zu EnCase entwickelte AccessData das Programm Forensic Toolkit (FTK), das sich ebenfalls als wichtiges digitalforensisches Analyseinstrument etablierte und insbesondere über ausgeprägte Indexierungs- und Suchfunktionen verfügte. Im deutschsprachigen Raum wird FTK beispielsweise auch heute noch von Steuerfahndungsbehörden eingesetzt.

Mit X-Ways Forensics entstand darüber hinaus ein europäisches Konkurrenzprodukt aus Deutschland, das sich vor allem bei deutschen Ermittlungsbehörden einer wachsenden Beliebtheit erfreute und bis heute erfreut. Unschlagbarer Vorteil von X-Ways ist bis zur aktuellen Version, dass es mit sehr geringen Anforderungen an die genutzte Hardware auskommt und nicht installiert werden muss.

Der Objektivität halber muss in diesem Kontext angeführt werden, dass in der Zeit auch das Zeitalter der technologischen Abhängigkeit von Anbietern in einem sehr engen Markt anbrach. Diese führt bis zum heutigen Tag dazu, dass jährlich erhebliche Summen für die Softwarepflege aufgewendet werden müssen.

Das erste DFRWS und die wissenschaftliche Grundlegung

Im August 2001 fand in Utica, New York, der erste Digital Forensic Research Workshop (DFRWS) statt – eine zweitägige Konferenz, die Wissenschaftler und Praktiker aus dem Bereich der digitalen Forensik zu einem offenen Austausch zusammenbrachte (Palmer, 2001). Seitdem hat sich das DFRWS zu einer der wichtigsten wissenschaftlichen Veranstaltungen in diesem Bereich entwickelt und findet nach wie vor jährlich statt.

Das erste DFRWS hatte eine wegweisende Bedeutung: Es definierte einen systematischen Forschungsplan für die digitale Forensik und klärte erstmals grundlegende Definitionsfragen (Palmer, 2001). Darüber hinaus wurden auch die Defizite der jungen Wissenschaft klar benannt: fehlende standardisierte Methoden, unzureichende Ausbildungsprogramme, mangelnde Möglichkeiten zur Validierung forensischer Tools sowie die Notwendigkeit, die Disziplin auf eine solide wissenschaftliche Grundlage zu stellen. Der DFRWS läutete damit das Ende der informellen Pionierphase ein und war der Startschuss auf dem Weg zur anerkannten wissenschaftlichen Disziplin.

Europol und die institutionelle europäische Zusammenarbeit

Nicht nur auf wissenschaftlicher Ebene wurde die Vernetzung professionalisiert, auch im Bereich der Strafverfolgung schritt die institutionelle europäische Zusammenarbeit voran. Europol – die europäische Polizeibehörde – hatte seine Wurzeln in einem Beschluss des EU-Gipfels von Maastricht im Jahr 1991 (BKA, n.d.-d). Nach einer mehrjährigen Vorbereitungsphase nahm Europol im Juli 1999 offiziell seine Tätigkeit auf, nachdem das Europol-Übereinkommen im Oktober 1998 in Kraft getreten war (BKA, n.d.-d).

Das ENFSI wurde 1999, nach Annahme seiner ersten Satzung, operational und begann mit dem Aufbau strukturierter Qualitätssicherungsmechanismen. Im Jahr 2003 verfügte ENFSI bereits über 49 Mitgliedsinstitute aus 33 europäischen Ländern und 15 aktive Expert Working Groups – darunter die Gruppe Forensic Information Technology (FIT) (ENFSI, 2020). Die ENFSI-FIT-Gruppe erarbeitete in diesen Jahren erste Leitlinien für die forensische Untersuchung von IT-Systemen und trieb damit die Professionalisierung maßgeblich voran.

Mobile Forensik: Eine neue Teildisziplin entsteht

Mit der zunehmenden Verbreitung von Mobiltelefonen in der Bevölkerung ab Ende der 1990er Jahre entstand eine neue Herausforderung für forensische Ermittler: die Auswertung mobiler Endgeräte. Als Teilgebiet der digitalen Forensik stammt die Mobilfunkforensik aus den späten 1990er und frühen 2000er Jahren. Die ersten Versuche, mobile Geräte zu untersuchen, erfolgten mit rudimentären Mitteln: Ermittler fotografierten den Bildschirminhalt ab oder nutzten handelsübliche Synchronisierungssoftware, um Gerätedaten zu sichern. Diese Methoden waren forensisch unzuverlässig, da die Synchronisierungssoftware in den Gerätespeicher schreiben und so Originaldaten verändern konnte. Im Kern handelte es sich zu diesem Zeitpunkt mehr um die Erstellung von „Backups“ als um eine forensisch korrekte Datenduplikation.

Im Jahr 2007 gründete das israelische Unternehmen Cellebrite seine Abteilung für mobile Forensik und stellte das Universal Forensic Extraction Device (UFED) vor – ein hardwaregestütztes Tool, das die Extraktion physischer und logischer Daten aus einer Vielzahl von Mobiltelefonen ermöglichte, einschließlich der Wiederherstellung gelöschter Daten (Cellebrite, 2021). UFED entstand aus einer Hard- und Softwarelösung zur Sicherung und Übertragung von Daten in Handy-Shops (als Service beim Neukauf eines Geräts) und avancierte in den folgenden Jahren zum De-facto-Industriestandard für die mobile Forensik bei Strafverfolgungsbehörden weltweit – auch in Deutschland, wo es bei den meisten forensischen Organisationseinheiten in Bund und Ländern eingesetzt wird.

Ungeachtet der weiteren Entwicklungen in der Mobilfunkforensik müssen auch heute noch viele Smartphones technisch bedingt im laufenden Betrieb (und damit nicht streng forensisch) gesichert werden.

Standardisierung und institutioneller Ausbau (2007–2015)

Diese Phase war geprägt von internationalen Normen und der weiteren institutionellen Konsolidierung. ISO-Standards schufen einen globalen Rahmen, während Europol und ENFSI ihre Position als zentrale Akteure festigten.

ISO/IEC 27037: Ein internationaler Rahmen für digitale Beweissicherung

Ein weiterer Meilenstein in der internationalen Standardisierung der digitalen Forensik war die Veröffentlichung der ISO/IEC 27037:2012 am 15. Oktober 2012 durch die International Organization for Standardization (ISO). Diese Norm definiert Leitlinien für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel und ist Teil der Normenfamilie ISO/IEC 27000 für Informationssicherheitsmanagementsysteme.

Kernaussage der ISO/IEC 27037 ist, dass für die Untersuchung digitaler Beweise eine Methode eingehalten werden muss, die geeignet ist, die Integrität und Beweiskraft aufrechtzuerhalten (ISO/IEC, 2012). Die Norm unterscheidet dabei zwischen verschiedenen Rollen im forensischen Prozess – dem First Responder am Tatort, dem Digital Forensic Practitioner im Labor und dem Sachverständigen vor Gericht. Diese Unterteilung wird heute unter anderem dafür genutzt, geeignete Aus- und Weiterbildungsangebote für die entsprechenden Zielgruppen zu definieren. In Deutschland wurde die internationale Norm als DIN EN ISO/IEC 27037:2016 übernommen und trägt seitdem zur Vereinheitlichung der forensischen Praxis bei (ISO/IEC, 2012). Sie bildet zusammen mit den Ergänzungsnormen ISO/IEC 27041, ISO/IEC 27042 und ISO/IEC 27043 den normativen Kern der internationalen digitalen Forensik.

Europol und das European Cybercrime Centre (EC3)

Im Januar 2013 nahm das European Cybercrime Centre (EC3) bei Europol in Den Haag seinen Betrieb auf. Seine Einrichtung war eine Priorität der EU-Strategie für innere Sicherheit. Das EC3 übernahm neben seiner Koordinierungsfunktion auch die Aufgabe, technische und digitale forensische Unterstützung für Ermittlungen der Mitgliedstaaten bereitzustellen. Bereits im

ersten Jahr seiner Tätigkeit führte das EC3 dedizierte Forensikschulungen durch, darunter im Mai 2013 ein Forensic Expert Training in Wiesbaden in enger Kooperation mit dem deutschen BKA. Im Jahr 2022 richtete Europol eine eigenständige Abteilung für digitale Forensik ein.

ENFSI als europäische Monopolorganisation

Die Europäische Kommission erkannte das ENFSI 2009 als Monopolorganisation für Forensikwissenschaft in Europa an und verpflichtete sich, es in allen Fragen der forensischen Wissenschaft zu konsultieren (ENFSI, 2020). 2015 wurde das ENFSI-Sekretariat von Polen nach Deutschland verlegt, was die zentrale Rolle Deutschlands im europäischen forensischen Netzwerk unterstreicht. Bis 2019 war die Mitgliedschaft des ENFSI auf 71 Laboratorien aus 39 europäischen Ländern angewachsen – von den ursprünglich 11 Gründungsmitgliedern aus dem Jahr 1993 (ENFSI, 2020).

Das BKA als Kompetenzzentrum: Das Kriminaltechnische Institut

Das Kriminaltechnische Institut (KTI) des BKA ist nach eigener Darstellung das Zentrum der fachlichen Expertise für die Sicherung, Untersuchung und Auswertung materieller Spuren (BKA, n.d.-e). Seit den frühen 2000er Jahren wuchs der Bereich der IT-Forensik innerhalb des KTI kontinuierlich. Zu den Kernaufgaben zählen Entwicklung und Test von Methoden und Werkzeugen zur Sicherung, Untersuchung, Sichtbarmachung, Aufbereitung und Bereitstellung digitaler Daten (BKA, n.d.-a). Das Spektrum der zu untersuchenden Beweisträger ist enorm vielfältig: Speicherkarten, Spielekonsolen, Chipkarten, optische Medien sowie Mobiltelefone und SIM-Karten (BKA, n.d.-a). Im Oktober 2007 bezog das KTI sein neues Laborgebäude in Wiesbaden mit 12.500 Quadratmetern Fläche für rund 340 Mitarbeiter (BKA, n.d.-b). Auch die Aufgaben haben sich seitdem mehrfach erweitert. So kamen beispielsweise Live-Forensik an laufenden Systemen oder Darknet-Forensik für die Ermittlung im TOR-Netzwerk dazu.

Neue Herausforderungen und Spezialisierung (2015–2022)

Mit der fortschreitenden Digitalisierung entstanden völlig neue forensische Felder. Cloud-Dienste, IoT-Geräte und vernetzte Fahrzeuge stellten die Behörden vor bisher unbekannte technische und rechtliche Probleme.

Gründung der ZITiS

Ein spezifisch deutsches Merkmal der institutionellen Entwicklung der digitalen Forensik ist die Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) am 6. April 2017. ZITiS hat als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern die Aufgabe, Bundesbehörden – insbesondere BKA, BfV und Bundespolizei – in informationstechnischen Fragen zu unterstützen. Zu den vier Aufgabenschwerpunkten zählen: digitale Forensik, Telekommunikationsüberwachung, Kryptoanalyse und Big-Data-Analyse. Wichtig ist die klare institutionelle Grenzziehung: ZITiS selbst hat keine polizeilichen Befugnisse und nimmt keine Ermittlungsaufgaben wahr – sie arbeitet ausschließlich als Forschungs- und Entwicklungsstelle. Die Gründung der ZITiS kann auch als Bestätigung gesehen werden, dass eigene staatliche Forschung (unter anderem) im Bereich digitale Fo-

rensik als unverzichtbar angesehen wird. Die ZITiS kooperiert dabei auch mit den europäischen Partnern, unter anderem im FORMOBILE-Projekt, um Forensikmethoden für Mobiltelefone in Strafprozessen zu standardisieren.

Cloud-Forensik: Der virtuelle Tatort

Die zunehmende Nutzung von Cloud-Diensten durch Privatpersonen und Unternehmen hat die digitale Forensik vor fundamental neue Herausforderungen gestellt. Während früher physische Datenträger beim Verdächtigen beschlagnahmt werden konnten, verteilt sich der „digitale Tatort" in der Cloud über verschiedene IT-Dienstleister und Serverstandorte – oft in unterschiedlichen Jurisdiktionen. Dabei ist nicht nur die Sicherung von Cloud-Daten technisch anspruchsvoller und erfordert spezielle Schnittstellen und Protokolle, darüber hinaus stellen sich auch komplexe internationale Rechtsfragen, da die Server von Cloud-Anbietern in vielen Fällen nicht (oder mindestens nicht alle) in Deutschland stehen. Die komplexen Zusammenhänge und die oft genutzten proprietären Techniken der Anbieter bringen es mit sich, dass bislang ausreichend standardisierte Verfahren für die Cloud-Forensik fehlen, was die Nachvollziehbarkeit der gewonnenen Beweise erschwert. Streng genommen fehlt es in dem Kontext schon an einer klaren und eindeutigen Definition der „Cloud", da sich hinter diesem Begriff etliche komplett unterschiedliche Dienste und Techniken verbergen.

IoT-Forensik und das erweiterte digitale Spurenbild

Das Internet of Things (IoT) – also die Vernetzung von Alltagsgegenständen über das Internet – hat die Menge potenzieller Beweisquellen für forensische Ermittler enorm erweitert. Smartwatches, vernetzte Haushaltsgeräte, Smart-TV-Systeme, Fitnesstracker oder Smart-Home-Steuerungen zeichnen kontinuierlich Daten über das Verhalten und die Aufenthaltsorte ihrer Nutzer auf. Für die Strafverfolgung ergeben sich daraus neue Ermittlungsansätze und neue Herausforderungen: Ein vernetzter Kühlschrank kann aufzeigen, wann jemand zu Hause war; eine Smartwatch speichert physiologische Daten bis hin zum Sterbezeitpunkt; Smart-TV-Protokolle können einen Hinweis auf den Aufenthaltsort zur Tatzeit geben. Gleichzeitig stellt die Heterogenität der Geräte, Betriebssysteme und Datenformate Forensiker vor erhebliche technische Herausforderungen. Erschwerend kommt noch hinzu, dass im Bereich IoT trotz Versuchen, industrieweit Standards anzubieten, von den Anbietern immer noch kaum einheitliche Techniken genutzt werden.

Das FORMOBILE-Projekt: Europäische Standardisierung der Mobilfunkforensik

Dass eine durchgehende Standardisierung für einen akzeptierten und funktionierenden forensischen Prozess unerlässlich ist, erkannte auch die Europäische Union: Das EU-Forschungsprojekt FORMOBILE (From Mobile Phones to Court) war in diesem Kontext ein wegweisendes Vorhaben zur europäischen Standardisierung der Mobilfunkforensik. Von Mai 2019 bis April 2022 arbeiteten 19 Partner aus 15 Nationen – darunter sieben Sicherheitsbehörden, vier Universitäten und Hochschulen sowie privatwirtschaftliche Unternehmen – mit einer Fördersumme von knapp 7 Millionen Euro aus dem EU-Forschungsprogramm Horizont 2020 zusammen (CORDIS, 2019; Hochschule Mittweida, 2022). Koordiniert wurde das Projekt von der Hochschule Mittweida. Das übergeordnete Ziel war die Etablierung einer

vollständigen forensischen Untersuchungskette für mobile Geräte über den ganzen forensischen Lebenszyklus – von der ersten Berührung des Telefons durch einen First Responder am Tatort bis zur Vorlage der Beweise vor Gericht (CORDIS, 2019).

Als zentrales Ergebnis des FORMOBILE-Projekts wurde der CEN Workshop Agreement (CWA 17865:2022) veröffentlicht – eine Vorstufe zu einem vollwertigen ISO-Standard (Ewald, 2024; Hochschule Mittweida, 2022). Dieser Standard adressiert alle Akteure der forensischen Prozesskette: Polizisten am Tatort, Analysten in forensischen Laboratorien, Strafverfolger und Staatsanwälte, Strafverteidiger und Richter (Hochschule Mittweida, 2022).

Aktuelle Entwicklungen und Ausblick

Die Gegenwart ist geprägt von rasanten technologischen Veränderungen. Künstliche Intelligenz, Big Data und neue Beweismittelkategorien wie Fahrzeuge oder Drohnen erweitern das Spektrum der digitalen Forensik kontinuierlich.

Künstliche Intelligenz in der digitalen Forensik

Neue Herausforderungen für die digitale Forensik entstanden durch die steigende Verbreitung von Methoden der Künstlichen Intelligenz (KI) und des maschinellen Lernens, mithin wichtige aktuelle Entwicklungen. KI-gestützte Analysesysteme können riesige Datenmengen verarbeiten, Muster erkennen und potenzielle Beweismittel mit deutlich höherer Geschwindigkeit und Genauigkeit identifizieren, als es manuell auch unter Einsatz einer riesigen Zahl an Forensikern oder Analysten möglich wäre. Konkrete Anwendungsfelder sind etwa die automatisierte Kategorisierung von Bild- und Videomaterial, die Gesichtserkennung zur Täteridentifikation sowie die Erkennung von Anomalien in Netzwerkverkehr oder Systemprotokollen. Nicht nur das BKA setzt KI-gestützte Werkzeuge zur Auswertung umfangreicher Datenbestände ein (BKA, n.d.-a).

Trotz aller Chancen bringt der KI-Einsatz auch neue Herausforderungen mit sich: Die Transparenz und Nachvollziehbarkeit der algorithmischen Analyseergebnisse ist bei vielen KI-Systemen noch unzureichend – eine Conditio sine qua non für die Gerichtsfestigkeit. Zudem werden Fragen der Datenschutzkonformität und der Fehleranfälligkeit forensischer Softwarewerkzeuge kritisch diskutiert. Bereits bekannt ist das Problem, dass Forensiksoftware gelegentlich Daten übersieht, falsch interpretiert oder fehlerhafte Ergebnisse liefert, was zu Fehlurteilen führen kann (Deutschlandfunk, 2021).

Nicht zuletzt können KI-Systeme auch zu Objekten forensischer Untersuchungen werden. Hierzu wäre ein tiefgehendes Verständnis der neuronalen Netze erforderlich, was derzeit in vielen Fällen aufgrund fehlender oder noch nicht abgeschlossener Forschung nicht möglich sein dürfte.

Automatisierung, Big Data und Kryptowährungsforensik

Eine weitere Herausforderung im forensischen Kontext sind die ständig wachsenden Datenmengen. Diese haben schon heute oft ein Ausmaß erreicht, das mit klassischen, manuellen forensischen Methoden kaum noch zu bewältigen ist. Moderne Smartphones können mehr als ein Terabyte an Daten enthalten; ambitionierte Privatanwender haben mehrere Terabyte an Speicher zu Hause und Cloud-Dienste können mehrere Petabyte umfassen. Der Betrieb großer Rechnersysteme zur Verarbeitung der Datenmengen ist heute schon in vielen Behörden üblich. Europol erforschte im Zuge seiner EncroChat-Auswertung ab 2020 die Nutzung von Machine-Learning-Modellen, um die Masse der zu prüfenden Nachrichten zu filtern (Netzpolitik, 2025).

Ein weiteres wichtiges Spezialgebiet, das in den letzten Jahren Einzug in forensische Untersuchungen gehalten hat, ist die Analyse von Kryptowährungstransaktionen. Täter nutzen Bitcoin, Monero und andere Kryptowährungen für Geldwäsche, Ransomware-Zahlungen oder den Handel auf illegalen Marktplätzen. Die forensische Analyse von Blockchain-Daten erfordert spezialisierte Tools und Methoden, die in den letzten Jahren erheblich weiterentwickelt wurden. BKA und Europol sind hier gleichermaßen aktiv.

Automotive Forensik: Das Fahrzeug als digitaler Tatort

Moderne Kraftfahrzeuge sind längst keine rein mechanischen Fortbewegungsmittel mehr, sondern hochkomplexe, vernetzte Datenverarbeitungssysteme. Ein aktuelles Fahrzeug verfügt über eine Vielzahl an unterschiedlichen Steuergeräten (Electronic Control Units, ECU), ein GPS-gestütztes Navigationssystem, ein Infotainmentsystem (oft mit Bluetooth-Kopplung und Anrufprotokollen) sowie seit einigen Jahren verpflichtend über einen Event Data Recorder (EDR). Für die digitale Forensik ergibt sich daraus eine neue Beweismittelkategorie, die in Ermittlungsverfahren zu Verkehrsunfällen, Fahrzeugdiebstahl, Mord oder Terrorismus zunehmend relevant wird.

Der EDR – im deutschen Sprachraum häufig als „Unfalldatenspeicher“ oder „Blackbox“ bezeichnet – speichert kontinuierlich Fahrdaten und überschreibt diese zyklisch. Im Moment eines Auslöseereignisses (typischerweise eine starke Verzögerung oder die Auslösung eines oder mehrerer Airbags) sichert das System rückwirkend die letzten fünf Sekunden sowie bis zu 0,3 Sekunden nach dem Ereignis. Gespeichert werden unter anderem Fahrgeschwindigkeit, Lenkwinkel, Brems- und Gaspedalstellung, Gurtstatus und Airbag-Aktivierung. Durch die EU-Verordnung 2019/2144 ist der EDR seit dem 6. Juli 2022 für alle neu typzugelassenen Fahrzeuge in der EU verpflichtend; seit dem 7. Juli 2024 gilt die Pflicht für alle neu zugelassenen Pkw. Diese Regelung schafft grundsätzlich eine verlässliche forensische Grundlage für Unfallrekonstruktionen und macht Deutschland und Europa zum Pionier in der regulatorischen Absicherung der Fahrzeugforensik, gleichzeitig werden aber auch neue Herausforderungen für Aus- und Weiterbildung von Forensikern geschaffen.

Neben dem EDR bieten Infotainmentsysteme eine weitere wertvolle Datenquelle: Gespeicherte GPS-Routen, gekoppelte Bluetooth-Geräte mit Gerätename und MAC-Adresse, Anruflisten, Kontaktlisten sowie Mediendateien können durch forensische Extraktion gewonnen werden. Die Hochschule Mittweida hat in Kooperation mit dem Fraunhofer SIT in ihrer

Forschungsarbeit „Das Auto als forensischer Datenspeicher“ dokumentiert, welche Datenkategorien in modernen Fahrzeugen anfallen und welche forensischen Methoden zu ihrer gerichtsverwertbaren Sicherung geeignet sind. Die Herausforderungen sind erheblich: Hersteller verwenden proprietäre Protokolle und Dateiformate, es fehlen branchenweit standardisierte Zugriffsverfahren und der Zugriff auf Fahrzeugdaten durch Polizeibehörden ist rechtlich uneinheitlich geregelt. Der europäische Dachverband DEKRA hat die EU-Gesetzgebung deshalb wiederholt aufgefordert, klare Vorschriften zu den Datenzugangsrechten für Fahrzeugprüfungsorganisationen, Strafverfolgungsbehörden und Unfallanalytiker zu schaffen (DEKRA, 2022). Das European Centre for Cybercrime Training and Education Group (ECTEG) trägt dem wachsenden Bedarf Rechnung und hat ein dediziertes Schulungsmodul zur Fahrzeugforensik (Vehicular Forensics) für europäische Strafverfolgungsbeamte entwickelt.

UAV-Forensik: Drohnen als Beweis- und Tatmittel

Unbemannte Luftfahrzeuge (Unmanned Aerial Vehicles, UAV) – im allgemeinen Sprachgebrauch als Drohnen bezeichnet – haben in den letzten Jahren sowohl die Möglichkeiten der Strafverfolgung als auch das kriminelle Handlungsrepertoire erheblich erweitert. Aus forensischer Sicht sind Drohnen in zweierlei Hinsicht relevant: als Tatmittel (z. B. zum Schmuggel von verbotenen Waren in Justizvollzugsanstalten, für Spionage oder terroristische Angriffe) sowie als Träger von beweiskräftigen Daten in den internen und externen Systemen.

Kommerzielle Drohnen – insbesondere die marktführenden Systeme des Herstellers DJI – speichern umfangreiche Flugdaten: GPS-Koordinaten von Start- und Landepunkten, vollständige Flugrouten, Zeitstempel, Kamera- und Videoaufnahmen sowie Fernsteuerungsparameter und weitere Telemetriedaten. Diese Daten verteilen sich auf verschiedene Speicherorte: den internen Flash-Speicher der Drohne, die eingesetzte Speicherkarte, das Steuerungsgerät (Fernbedienung oder Smartphone-App) sowie ggf. die Cloudspeicher des Herstellers. Nicht in allen Fällen können die Daten mittels standardisierter Methoden oder kommerziell verfügbarer Tools extrahiert werden.

Deutlich größere forensische Herausforderungen stellen selbst gebaute Drohnen dar, da diese aus heterogenen Komponenten unterschiedlicher Hersteller bestehen können und nicht zwingend eine einheitliche Datenstruktur aufweisen. Das Bundesministerium für Bildung und Forschung (BMBF) förderte deshalb von 2022 bis 2025 das Forschungsprojekt FOCUS (Forensische Untersuchung von Selbstbaudrohnen), an dem die Universität der Bundeswehr München als Koordinatorin, das Bundeskriminalamt (BKA), die ZITiS sowie das Hessische Landeskriminalamt beteiligt waren. Ziel des Projekts war die Entwicklung strukturierter forensischer Untersuchungsmethoden für Selbstbaudrohnen. Die Ergebnisse wurden 2025 in der TIB-Forschungsdatenbank veröffentlicht und bilden eine erste deutsche Grundlage für standardisierte forensische Methoden in Bezug auf UAV. Ergänzend hat die amerikanische Scientific Working Group on Digital Evidence (SWGDE) 2022 ihre Best Practices for Drone Forensics veröffentlicht, die international als Orientierungsrahmen dienen (SWGDE, 2022).

Akademische Ausbildungswege in Deutschland

Begleitend zur technischen Professionalisierung der digitalen Forensik entstand in Deutschland ein spezialisiertes akademisches Ausbildungsangebot. Die Hochschule Mittweida bietet sowohl einen Bachelorstudiengang IT-Forensik/Cybercrime als berufsbegleitendes Fernstudium als auch einen grundständigen Bachelorstudiengang Allgemeine und Digitale Forensik an, der Informatikkenntnisse mit naturwissenschaftlich-forensischen Methoden verknüpft (Hochschule Mittweida, n.d.-a; Hochschule Mittweida, n.d.-b). Weitere Ausbildungsangebote existieren an der Hochschule Fresenius (Idstein), der Technischen Hochschule Brandenburg und anderen Hochschulen in Deutschland (Studis Online, n.d.). Diese akademischen Programme ergänzen die polizeiinterne Aus- und Fortbildung, die beim BKA durch das KTI koordiniert wird.

Rechtsrahmen und normative Entwicklung

Trotz technischer Fortschritte hinkt die Gesetzgebung oft hinterher. Dieser Abschnitt beleuchtet die Spannung zwischen Ermittlungsbedarf und Grundrechten sowie die Bemühungen um europäische Harmonisierung.

Strafprozessrechtliche Entwicklungen

Das deutsche Straf- und Strafprozessrecht hat auf die Herausforderungen der digitalen Forensik bisher nur punktuell und ohne systemische Reform reagiert. Die §§ 94 ff. StPO bleiben die wesentliche Rechtsgrundlage für die Sicherstellung und Beschlagnahme digitaler Beweismittel. Diese Vorschriften, die seit 1879 nicht wesentlich weiterentwickelt wurden, sind auf die besonderen Eigenschaften digitaler Daten nicht zugeschnitten (BVerfG, 2005). Die hohe Streubreite des Informationsgehalts eines Datenträgers erfordert nach der Rechtsprechung des BVerfG eine gezielte Auswahl relevanter Daten und weitgehenden Schutz nicht verfahrensrelevanter Informationen (BVerfG, 2005). Das durch diese Entscheidung entstehende Spannungsfeld zwischen dem Ermittlungsinteresse und dem informationellen Selbstbestimmungsrecht des Betroffenen bleibt eine zentrale Herausforderung.

Europäische Harmonisierung

Auf europäischer Ebene hat die Europäische Union die Notwendigkeit harmonisierter Standards für digitale Beweismittel erkannt. Mit dem FORMOBILE-Projekt wurde ein erster Schritt in Richtung eines EU-weiten Standards für die Mobilfunkforensik unternommen (Hochschule Mittweida, 2022; Ewald, 2024). Langfristig strebt die EU eine weitergehende Harmonisierung der forensischen Standards an, um die grenzüberschreitende Zusammenarbeit zu erleichtern. Die Anerkennung des ENFSI durch die Europäische Kommission im Jahr 2009 als monopolistischen Ansprechpartner für forensische Wissenschaftsfragen stärkt die Normierungsarbeit gegenüber den nationalen Behörden erheblich (ENFSI, 2020).

Fazit

Die digitale Forensik hat in den betrachteten gut drei Jahrzehnten seit den frühen 1990er Jahren einen bemerkenswerten Weg von der informellen Praxis einzelner computerkundiger Ermittler zu einer wissenschaftlichen Disziplin zurückgelegt, die international standardisiert, akademisch verankert und institutionell fest etabliert ist. In Deutschland hat das BKA mit seinem Kriminaltechnischen Institut eine führende Rolle gespielt und war früh an der europäischen Vernetzung beteiligt. Die Gründung der ZITiS im Jahr 2017 zeigt beispielhaft, dass dieser Prozess bis in die jüngste Vergangenheit andauert und nicht nur technisch, sondern auch organisatorisch auf die Herausforderungen reagiert werden muss und wird.

Auf europäischer Ebene haben die Gründung des ENFSI im Jahr 1995 und seines FIT-Arbeitsbereichs 1998, die Anerkennung durch die EU-Kommission 2009 sowie die Etablierung des EC3 bei Europol 2013 einen stabilen institutionellen Rahmen für die europäische forensische Zusammenarbeit geschaffen. Das FORMOBILE-Projekt hat gezeigt, dass auch komplexe forensisch-technische Standardisierungsprobleme im europäischen Forschungskonsortium erfolgreich angegangen werden können.

Die technischen Herausforderungen der kommenden Jahre – Cloud-Forensik, IoT-Forensik, KI-gestützte Analyse, Blockchain-Auswertung, die zunehmende Datenmenge und die zunehmende Digitalisierung allgemein – sind erheblich. Sie erfordern eine kontinuierliche Anpassung der Methoden, Werkzeuge und rechtlichen Rahmenbedingungen. Gleichzeitig bleibt der Grundsatz unverändert, der seit den ACPO-Leitlinien von 1998 und der ISO/IEC 27037:2012 das Fundament der digitalen Forensik bildet: Die Integrität der Beweismittel muss durch wissenschaftlich anerkannte, nachvollziehbare und reproduzierbare Methoden gewährleistet sein.

Für die sprachliche Überarbeitung und die Prüfung der Quellenformatierung wurden KI-Modelle eingesetzt.

Referenzen

Association of Chief Police Officers. (1998). ACPO good practice guide for computer based electronic evidence (1. Aufl.). ACPO.

Bundeskriminalamt. (n.d.-a). IT-Forensik: Spurensuche in Bits und Bytes. https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik.html

Bundeskriminalamt. (n.d.-b). History of the Forensic Science Institute. https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/ForensicScience/History/history.html

Bundeskriminalamt. (n.d.-c). Erkennungsdienst. https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst.html

Bundeskriminalamt. (n.d.-d). Europol – Geschichte und Aufgaben. https://www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/InternationaleFunktion/Europol/europol.html

Bundeskriminalamt. (n.d.-e). Abteilung „Kriminaltechnisches Institut“ (KTI). https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/KriminaltechnischesInstitut/kriminaltechnischesinstitut_node.html

Bundesverfassungsgericht. (2005). Beschluss des Zweiten Senats vom 12. April 2005 – 2 BvR 1027/02. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2005/04/rs20050412_2bvr102702.html

Cellebrite. (2021). The solution that changed modern digital investigations forever. https://cellebrite.com/en/blog/the-solution-that-changed-modern-digital-investigations-forever/

Cilip. (2020). Von der Kartei zum Datenhaus: Eine kleine Geschichte polizeilicher Datenhaltung. https://www.cilip.de/2020/05/05/von-der-kartei-zum-datenhaus-eine-kleine-geschichte-polizeilicher-datenhaltung/

CORDIS. (2019). FORMOBILE: A complete forensic investigation chain targeting mobile devices (Projektnummer 832800). Europäische Kommission. https://cordis.europa.eu/project/id/832800/de

Dewald, M. (2015). Forensische Informatik: Grundlagen und Anwendungen. Springer Vieweg.

European Network of Forensic Science Institutes. (2020). ENFSI history and membership. https://enfsi.eu/about-us/history/

Europol. (2013). EC3 first year report. https://www.europol.europa.eu/cms/sites/default/files/documents/ec3_first_year_report.pdf

Guidance Software. (2012). Guidance Software celebrates its 15th anniversary. MarketScreener. https://in.marketscreener.com/quote/stock/GUIDANCE-SOFTWARE-INC-39131/

Hochschule Mittweida. (2022, Juli 12). Fokus Forschung: Erfolgreiches EU-Projekt FORMOBILE geht zu Ende. https://www.forschung.hs-mittweida.de/news/aktuell/7461/

International Organization for Standardization. (2012). ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. https://www.iso.org/standard/54534.html

Kopp, I., & Sprangers, W. (2002). History of European Network of Forensic Science Institutes. Problems of Forensic Sciences, 50(L), 203–217.

National Institute of Standards and Technology. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final

Open University. (n.d.). 4.2 A brief history of digital forensics. OpenLearn. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2

Palmer, G. L. (2001). A road map for digital forensic research: Report from the First Digital Forensic Research Workshop. Digital Forensic Research Workshop. https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

Laura Iva Savić . (2019). Die digitale Dimension des Strafprozessrechts: Zur Doppelnatur digitaler Beweise. Peter Lang Verlag.

Polizeigeschichte NRW. (2023). Chronik Polizeigeschichte NRW: 90er Jahre. https://www.polizeigeschichte-infopool.de/chronik-polizeigeschichte-nrw/90er-jahre/

Scientific Working Group on Digital Evidence. (2022). Best practices for drone forensics (Version 1.0). https://www.swgde.org/wp-content/uploads/2022/01/13-SWGDE-Best-Practices-for-Drone-Forensics_v1.0.pdf

Universität der Bundeswehr München. (n.d.). FOCUS – Forensische Untersuchung von Selbstbaudrohnen. https://www.unibw.de/digfor/forschung/focus

Der digitale Zwilling in der Forensik – Entstehung, Entwicklung und Bedeutung für die Polizeitechnik

Dirk Labudde

Die fortschreitende Digitalisierung hat die Polizeitechnik und insbesondere die forensische Tatortarbeit in den letzten Jahrzehnten grundlegend verändert. Während die klassische Tatortdokumentation lange Zeit auf zweidimensionale Fotografien, Skizzen und schriftliche Protokolle beschränkt war, ermöglichen moderne digitale Technologien heute eine nahezu vollständige, dreidimensionale Erfassung realer Tatorte. In diesem Zusammenhang hat sich zunehmend der Begriff des „forensischen digitalen Zwillings“ etabliert. Der digitale Zwilling beschreibt dabei nicht nur ein digitales Modell, sondern ein umfassendes, maßstabsgetreues und dauerhaft nutzbares digitales Abbild eines realen Tatortes oder Objektes. Eine konsequente Weiterentwicklung ist die Einbeziehung gekoppelter Systeme, was zum Konzept des Forensiums führt.

Dieses Kapitel zeichnet die historische und technische Entwicklung dieses Konzepts in der Forensik nach und ordnet dessen Bedeutung für die moderne Polizeitechnik ein.

Die Entwicklung der forensischen Fotografie und Tatortrekonstruktion im 21. Jahrhundert ist das Ergebnis eines langen Transformationsprozesses, der von der klassischen kriminalistischen Dokumentation über digitale Modellierung bis hin zu immersiven und KI-gestützten Analyseverfahren reicht. Was im 19. Jahrhundert als standardisierte Identifikationsfotografie begann, hat sich zu einem datengetriebenen, multidimensionalen Rekonstruktionssystem entwickelt, das physische, chemische und digitale Spuren in einem integrativen Modell vereint.

Zwischen 1995 und 2010 entstanden erste digitale Vorläufer des späteren digitalen Zwillings in der Forensik. Mit der Einführung digitaler Fotografie sowie CAD-gestützter Rekonstruktionen wurden Tatorte zunehmend digital dokumentiert. Diese frühen virtuellen Rekonstruktionen und digitalen Tatortmodelle dienten vor allem der Veranschaulichung, erfüllten jedoch noch nicht die Kriterien eines digitalen Zwillings, da eine vollständige 3D-Erfassung, eine konsistente Datenbasis und reproduzierbare Analysen fehlten.

Ab etwa 2010 führte der Einsatz moderner 3D-Erfassungstechnologien wie Laserscanning, Photogrammetrie, 360°-Kameras und Drohnen zu einem deutlichen Entwicklungsschub. Tatorte konnten nun nahezu vollständig, maßhaltig und realitätsnah erfasst sowie virtuell begangen werden. Der Begriff des „virtuellen Tatortes“ etablierte sich, während der Ausdruck „digitaler Zwilling“ noch zurückhaltend verwendet wurde.

Erst ab etwa 2016 setzte sich der Begriff „digitaler Zwilling“ im forensischen Kontext durch. Digitale Tatortabbilder erfüllten nun alle wesentlichen Merkmale eines digitalen Zwillings, darunter vollständige Geome-trie, Maßhaltigkeit, Datenintegration, langfristige Speicherung sowie Analyse- und Präsentationsmöglichkeiten. Der digitale Zwilling entwickelte sich damit von einer reinen Visualisierung zu einem eigenständigen, anerkannten Arbeits- und

Beweismittel in der Forensik. In den 2020er Jahren wurde der digitale Zwilling durch die Integration in den hypothesengetriebenen Ermittlungsprozess und dem Einsatz von intelligenten Systemen zu einem forensischen digitalen Zwilling.

Es lässt sich festhalten, dass vom digitalen Zwilling in der Forensik seit etwa 2016–2018 gesprochen wird. Erst mit den technischen Möglichkeiten, Tatorte vollständig, maßstabsgetreu und dauerhaft digital abzubilden, erfüllte das forensische Tatortmodell die Kriterien eines digitalen Zwillings. Der digitale Zwilling stellt heute einen wesentlichen Fortschritt in der Polizeitechnik dar und trägt entscheidend zu einer objektiven, reproduzierbaren und rechtssicheren Tatortarbeit bei.

Die einschlägige Literatur zur Tatortdokumentation weist drei zentrale Entwicklungslinien auf: Erstens die Digitalisierung klassischer Fotografie, die in Photogrammetrie und 3D-Scanning mündet und den Tatort geometrisch rekonstruierbar macht. Zweitens die spektrale Erweiterung durch multispektrale und hyperspektrale Verfahren, die Spuren jenseits des sichtbaren Lichts analysierbar machen. Drittens die Integration immersiver Technologien und Künstlicher Intelligenz, etwa durch Virtual Reality, Neural Radiance Fields und Deep Learning, die interaktive und algorithmisch gestützte Auswertungen ermöglichen. Insgesamt transformiert sich forensische Fotografie damit von einer primär dokumentarischen Technik zu einem datengetriebenen, modellbasierten Analyse- und Simulationsinstrument.

Die Entwicklung der forensischen Fotografie: Von der kriminalistischen Dokumentation zur digitalen Rekonstruktionswissenschaft

Die forensische Fotografie ist seit ihrer Einführung im 19. Jahrhundert ein zentrales Instrument kriminalistischer Dokumentation und Beweissicherung. Ihre Entwicklung spiegelt nicht nur den technologischen Fortschritt fotografischer Verfahren wider, sondern auch den Wandel kriminalistischer Methodik insgesamt. Von den ersten systematisierten Täterporträts bis hin zu dreidimensionalen, KI-gestützten Tatortrekonstruktionen hat sich die Rolle der Fotografie von einem dokumentarischen Hilfsmittel zu einem integrativen Analysewerkzeug erweitert.

Die Anfänge: Standardisierung und Identifikation im 19. Jahrhundert

Die Geburtsstunde der forensischen Fotografie ist eng mit dem Namen Alphonse Bertillon verbunden. Mit seinem Werk La photographie judiciaire (1890) etablierte Bertillon erstmals ein standardisiertes Verfahren zur fotografischen Erfassung von Tatverdächtigen (Bertillon, 1890). Die Einführung des sogenannten „Mugshots“ – einer normierten Kombination aus Frontal- und Profilaufnahme – war nicht nur ein technischer Fortschritt, sondern Ausdruck einer methodischen Revolution: Fotografie wurde systematisch in den kriminalistischen Identifikationsprozess integriert.

Parallel dazu entwickelte Hans Gross in seinem Handbuch für Untersuchungsrichter (1893) die Fotografie als Bestandteil einer wissenschaftlich fundierten Kriminalistik weiter (Gross, 1893). Gross erkannte früh, dass fotografische Dokumentation Objektivität versprach und

subjektive Wahrnehmung des Ermittlers ersetzen oder zumindest ergänzen konnte. Die Fotografie wurde damit Teil einer Beweislogik, die auf Reproduzierbarkeit und Nachvollziehbarkeit abzielte.

Im Zentrum dieser frühen Phase stand die Identifikation von Personen. Tatortfotografie im engeren Sinne entwickelte sich erst später systematisch. Dennoch wurde bereits hier deutlich, dass fotografische Verfahren eine neue Form der „visuellen Evidenz“ schufen, die in Gerichtsverfahren zunehmend an Bedeutung gewann.

Die analoge Tatortfotografie im 20. Jahrhundert

Im Verlauf des 20. Jahrhunderts wurde die Fotografie zu einem festen Bestandteil kriminalistischer Tatortarbeit. Mit der Verfügbarkeit tragbarer Kameras, verbesserter Objektive und empfindlicherer Filme konnte der Tatort zunehmend vollständig dokumentiert werden. Die Entwicklung standardisierter Aufnahmeschemata – Übersichtsaufnahme, Mittelaufnahme, Detailaufnahme – prägte die kriminaltechnische Ausbildung nachhaltig.

Moderne Lehrwerke wie jene von Robinson (2010) und Nafte (2009) systematisieren diese Vorgehensweise und betonen die Bedeutung strukturierter Bildfolgen für die spätere Rekonstruktion von Ereignisabläufen. Die analoge Tatortfotografie war dabei primär dokumentarisch orientiert: Ziel war die möglichst unverfälschte Sicherung des Ist-Zustandes zum Zeitpunkt der Aufnahme. Perspektivkorrekturen, Maßstabsleisten und Beleuchtungstechniken dienten der Sicherung der Beweisqualität.

Gardner und Krouskup (2018) beschreiben die Fotografie in dieser Phase als integralen Bestandteil der „Crime Scene Processing“-Prozedur. Sie war nicht isoliertes Medium, sondern eingebettet in Spurensicherung, Vermessung und kriminalistische Analyse. Die Beweiskraft fotografischer Dokumentation beruhte dabei auf ihrer vermeintlichen Objektivität – einer Eigenschaft, die im digitalen Zeitalter zunehmend kritisch hinterfragt wird.

Der Übergang zur digitalen Fotografie

Mit dem Einzug digitaler Kameratechnik in den 1990er und frühen 2000er Jahren begann ein fundamentaler Wandel. Digitale Bildsensoren ersetzten chemische Filmentwicklung, Speichermedien lösten Negative ab, und Bilddaten wurden manipulierbar. Dieser Paradigmenwechsel stellte die forensische Praxis vor neue Herausforderungen.

Während die digitale Fotografie erhebliche Vorteile bot – sofortige Bildkontrolle, verlustfreie Vervielfältigung, Metadatenspeicherung –, entstand zugleich die Notwendigkeit strenger Dokumentations- und Integritätsverfahren. Die Sicherung von Originaldateien, Hashwerten und Metadaten wurde Teil der Beweiskette. Saferstein (2020) betont in diesem Zusammenhang, dass digitale Bilddaten zwar eine höhere Flexibilität erlauben, jedoch neue Anforderungen an Authentizität und Nachvollziehbarkeit stellen.

Die Digitalisierung ermöglichte zugleich neue Analyseformen. Bildbearbeitungssoftware konnte Kontraste verstärken, Details hervorheben oder latente Spuren sichtbar machen. Damit begann sich die Rolle der Fotografie von einer rein dokumentarischen Technik hin zu einem analytischen Werkzeug zu verschieben.

Photogrammetrie und 3D-Rekonstruktion

Ein entscheidender Entwicklungsschritt war die Integration photogrammetrischer Verfahren in die forensische Praxis. Photogrammetrie nutzt überlappende Fotografien zur Berechnung dreidimensionaler Modelle. Urbanová et al. (2015) zeigen, dass sich mit dieser Methode kostengünstige und präzise 3D-Rekonstruktionen von Tatorten und Objekten erstellen lassen.

Carew, Morgan und Rando (2021) beschreiben diese Entwicklung als Entstehung einer eigenständigen „3D Forensic Science". Dreidimensionale Dokumentation erlaubt nicht nur Visualisierung, sondern exakte Vermessung von Spurenrelationen, Schusswinkeln oder Verletzungsmustern. Der Tatort wird damit in einen digitalen Datenraum transformiert, der unabhängig vom physischen Original analysiert werden kann.

Bereits Thali, Braun und Dirnhofer (2003) zeigten die Potenziale optischer 3D-Oberflächendigitalisierung in der forensischen Medizin. Diese frühen Arbeiten legten den Grundstein für heutige hochauflösende Laserscans und strukturierte Lichtverfahren.

Mit LiDAR- und strukturierten Lichtscannern lassen sich heute komplette Tatorte binnen Minuten millimetergenau erfassen (Richards & Siebert, 2017). Besonders bemerkenswert ist die zunehmende Verfügbarkeit mobiler LiDAR-Sensoren in Konsumgeräten, wodurch die 3D-Dokumentation demokratisiert wird.

Multispektrale und hyperspektrale Bildgebung

Parallel zur räumlichen Erweiterung entwickelte sich eine spektrale Erweiterung der forensischen Fotografie. Multispektrale und hyperspek- trale Bildgebung ermöglichen die Analyse von Spuren außerhalb des sichtbaren Lichtspektrums.

Edelman, van Leeuwen und Aalders (2012) demonstrieren, wie hyperspektrale Verfahren Blutspuren oder chemische Rückstände berührungslos identifizieren können. De Castro et al. (2018) zeigen darüber hinaus die Bedeutung von UV- und Infrarotfotografie zur Sichtbarmachung latenter Spuren.

Damit erweitert sich der fotografische Blick vom Sichtbaren zum Unsichtbaren. Fotografie ist nicht mehr bloß Abbildung, sondern spektrale Analyseplattform.

KI und modellbasierte Rekonstruktion

Mit der Integration Künstlicher Intelligenz beginnt eine weitere Entwicklungsstufe. Malik et al. (2024) untersuchen den Einsatz von Neural Radiance Fields (NeRF) zur Rekonstruktion komplexer Szenen aus Videomaterial. Diese Technik erlaubt fotorealistische, frei navigierbare 3D-Modelle.

Zappalà et al. (2024) kombinieren Deep Learning mit Virtual Reality, sodass Tatorte automatisiert analysiert und immersiv erfahrbar gemacht werden. Fotografie wird hier zur Datengrundlage algorithmischer Interpretation.

Die Studie zu Extended Reality Technologies (Technologies, 2024) zeigt, dass VR, AR und MR neue Formen der Präsentation und Analyse ermöglichen. Ermittler können Tatorte virtuell begehen und Hypothesen simulieren.

Von der Dokumentation zur Simulation

Die Entwicklung der forensischen Fotografie lässt sich somit als Übergang von der statischen Dokumentation zur dynamischen Simulation beschreiben. Während Bertillon (1890) die Standardisierung der Identifikationsfotografie etablierte und Gross (1893) die wissenschaftliche Methodik begründete, transformieren heutige 3D- und KI-Systeme den Tatort in ein digitales Modell. Carew et al. (2021) betonen, dass 3D-Forensik nicht nur technologische Innovation, sondern auch methodische Neuausrichtung bedeutet. Der Tatort ist nicht länger ausschließlich physischer Raum, sondern datenbasierte Rekonstruktion.

Gleichzeitig bleibt die Herausforderung der Validierung bestehen. Digitale Manipulierbarkeit, algorithmische Intransparenz und Fragen der gerichtlichen Zulässigkeit erfordern klare Standards.

Die Entwicklung der forensischen Fotografie ist geprägt von drei zen-tralen Transformationen:

1. Standardisierung und Objektivierung (19.–20. Jahrhundert)
2. Digitalisierung und 3D-Modellierung (spätes 20. – frühes 21. Jahrhundert)
3. Algorithmisierung und Immersion (Gegenwart)

Was als visuelles Hilfsmittel begann, ist heute integraler Bestandteil datengetriebener Tatortrekonstruktion. Dennoch bleibt der methodische Kern unverändert: Fotografie dient der Sicherung, Strukturierung und Bewertung von Spuren.

Die Zukunft der forensischen Fotografie liegt nicht allein in höherer Auflösung oder komplexeren Algorithmen, sondern in der Integration technischer Innovation mit kriminalistischer Logik.

Die Dokumentation von Tatorten hat sich in der Polizeitechnik von einfachen fotografischen Verfahren hin zu hochspezialisierten, digitalen und dreidimensionalen Aufnahmetechniken entwickelt. Ziel dieser Entwicklung ist eine möglichst objektive, nachvollziehbare und gerichtsfeste Sicherung von Spuren und Tatorten. Siehe dazu Abbildung 1.

Abb. 1: Zeitstrahl: Der Zeitstrahl zeigt chronologisch die Entwicklung der Kameratechnik in der Polizeitechnik

1. Frühe Phase: Klassische Fotografie (ab ca. 1900). Die ersten Tatortaufnahmen erfolgten mit analogen Kameras und Schwarz-Weiß-Fotografie. Der Schwerpunkt lag auf Übersichts- und Detailaufnahmen zur visuellen Dokumentation. Diese Technik bildet bis heute die Grundlage der Tatortarbeit, inzwischen überwiegend in digitaler Form. Anwendung: Tatortübersichten, Spurendokumentation, Beweisführung.

2. Erweiterung des sichtbaren Spektrums: UV- und IR-Fotografie (ab ca. 1960–1980). Mit Ultraviolett- und Infrarotkameras konnten erstmals Spuren sichtbar gemacht werden, die dem menschlichen Auge verborgen bleiben. Besonders biologische Spuren ließen sich auch nach Reinigungsversuchen nachweisen. Anwendung: Auffinden verdeckter Blutspuren, Material- und Faserunterschiede.

3. Thermische Verfahren: Wärmebildkameras (ab ca. 1990). Wärmebildkameras stellen Temperaturunterschiede dar und werden in der Polizeitechnik zur zeitnahen Tatortanalyse sowie bei Dunkelheit eingesetzt. Anwendung: Frische Fußspuren, kürzlich bewegte Gegenstände, Leichenauffindung.

4. Detailorientierung: Makro- und Mikroskopkameras (ab ca. 1990–2000). Diese Kameras ermöglichen hochauflösende Nahaufnahmen kleinster Spuren und sind insbesondere für die kriminaltechnische Spurensicherung von Bedeutung. Anwendung: Werkzeug-, Schuh- und Reifenspuren, Fasern, Haare.

5. Räumliche Erfassung: 3D-, Stereo- und 360°-Kameras (ab ca. 2005).

Durch räumliche Kamerasysteme wurde eine dreidimensionale Darstellung von Tatorten möglich, einschließlich virtueller Begehungen. Anwendung: Unfallaufnahme, Rekonstruktion, Schulung.

6. Mobile Übersicht: Drohnenkameras (ab ca. 2010). Drohnen mit hochauflösenden Kameras ermöglichen eine schnelle und großflächige Tatortübersicht, insbesondere im Außenbereich. Anwendung: Verkehrsunfälle, große Tatorte, Vermessung.

7. Moderne Entwicklungen: Multispektral-, Hyperspektral- und KI-gestützte Kameras (ab ca. 2015). Moderne Systeme kombinieren mehrere Spektralbereiche und nutzen KI zur Unterstützung bei Analyse und Rekonstruktion. Anwendung: Automatisierte Spurenerkennung, Beweisvisualisierung.

Fazit: Die Kameratechnik in der Polizeitechnik entwickelte sich von der zweidimensionalen Fotografie hin zu multispektralen und dreidimensionalen Systemen. Moderne Kameras ergänzen sich.

Crime Scene Reconstruction zwischen 3D-Modellierung, KI und Extended Reality

Die Rekonstruktion von Tatorten hat sich in den vergangenen zwei Jahrzehnten von einer primär kriminalistischen Disziplin hin zu einem hochgradig interdisziplinären Forschungsfeld entwickelt, in dem klassische Spurensicherung, naturwissenschaftliche Analytik, digitale Modellierung und immersive Visualisierungstechnologien zunehmend miteinander verschmelzen. Eine aktuelle systematische Bestandsaufnahme liefert die Scoping-Review von Balbudhe et al. (2025), die Crime Scene Reconstruction (CSR) als einen strukturierten Prozess definieren, der physische, biologische, chemische und digitale Spuren integriert, um Ereignisabläufe evidenzbasiert zu rekonstruieren. Die Autoren betonen, dass moderne Tatortrekonstruktion nicht mehr ausschließlich retrospektive Rekonstruktion bedeutet, sondern zunehmend datengetriebene Modellierung umfasst, bei der digitale Werkzeuge die Hypothesenbildung unterstützen. Dabei wird deutlich, dass insbesondere Standardisierung, Validierung und interdisziplinäre Zusammenarbeit zen-trale Herausforderungen der aktuellen Forschung darstellen (Balbudhe et al., 2025).

Parallel zu dieser methodischen Ausdifferenzierung hat sich mit der sogenannten „3D Forensic Science“ ein neues Teilgebiet etabliert. Carew, Morgan und Rando (2021) beschreiben 3D-Forensik als eigenständiges Feld, das 3D-Bildgebung, digitale Modellierung und computergestützte Analyse integriert. Hierzu zählen Laserscanning, Photogrammetrie, strukturierte Lichtverfahren sowie volumetrische Datenerfassung. Die Autoren argumentieren, dass dreidimensionale Dokumentationsverfahren nicht nur eine realitätsnahe Visualisierung ermöglichen, sondern auch messbare, reproduzierbare und gerichtsfeste Analysen unterstützen. Besonders hervorgehoben wird die Möglichkeit, komplexe Tatorte virtuell begehbar zu machen und Spurenrelationen in ihrer räumlichen Dimension nachvollziehbar darzustellen

(Carew et al., 2021). Damit verschiebt sich der Tatort zunehmend in einen digitalen Repräsentationsraum, der sowohl für Ermittlungsarbeit als auch für Gerichtsverfahren neue didaktische und argumentative Möglichkeiten eröffnet.

Bereits frühere Arbeiten zur 3D-Rekonstruktion betonten technische und gestalterische Anforderungen an solche Systeme. Bostanci (2015) diskutierte Designüberlegungen bei der 3D-Rekonstruktion von Tatorten und identifizierte Faktoren wie Genauigkeit, Benutzerfreundlichkeit, Datenintegrität und Interoperabilität als zentrale Qualitätskriterien. Schon hier wurde deutlich, dass 3D-Rekonstruktionen nicht lediglich Visualisierungshilfen sind, sondern strukturierte Datenmodelle darstellen, die forensisch belastbar sein müssen. Die Frage nach der Beweisqualität digitaler Modelle zieht sich seitdem als roter Faden durch die Forschung.

Mit dem Aufkommen immersiver Technologien wurde die dreidimensionale Tatortrekonstruktion weiterentwickelt. Die Studie „Extended Reality Technologies: Transforming the Future of Crime Scene Investigation“ (2024) beschreibt, wie Virtual Reality (VR), Augmented Reality (AR) und Mixed Reality (MR) neue Formen der Tatortanalyse ermöglichen. Extended-Reality-Systeme erlauben es Ermittlern, Sachverständigen und Gerichten, Tatorte interaktiv zu begehen, Hypothesen zu simulieren und alternative Szenarien zu testen. Dabei wird argumentiert, dass immersive Technologien nicht nur der Visualisierung dienen, sondern auch kognitive Prozesse unterstützen, indem sie räumliches Verständnis und Situationsbewusstsein verbessern (Technologies, 2024). Gleichzeitig weisen die Autoren auf Herausforderungen hinsichtlich Standardisierung, Datenvolumen, Hardwareanforderungen und juristischer Akzeptanz hin.

Einen weiteren Innovationsschub erhält das Feld durch die Integration von Deep Learning und KI-gestützten Analysen. Zappalà et al. (2024) zeigen, wie Virtual-Reality-Umgebungen mit Deep-Learning-Algorithmen kombiniert werden können, um Tatorte automatisiert zu analysieren. KI-Systeme unterstützen dabei etwa die Objekterkennung, Spurenklassifikation oder die Identifikation relevanter Muster in komplexen Szenarien. Die Autoren argumentieren, dass diese Verbindung von immersiver Darstellung und algorithmischer Auswertung eine neue Qualität der Tatortanalyse schafft, da visuelle Exploration und datengetriebene Mustererkennung simultan erfolgen können (Zappalà et al., 2024). Die Rolle des Ermittlers verändert sich dabei vom reinen Spurensicherer hin zum kuratierenden Analysten, der KI-generierte Vorschläge bewertet und kontextualisiert.

Einen technologisch besonders innovativen Ansatz verfolgen Malik et al. (2024) mit der Untersuchung der Machbarkeit sogenannter Neural Radiance Fields (NeRF) für die Tatortvideorekonstruktion. NeRF-Modelle ermöglichen die Rekonstruktion realistischer 3D-Szenen aus zweidimensionalen Bild- oder Videodaten, indem neuronale Netze Licht- und Raumverhältnisse modellieren. Die Autoren zeigen, dass sich mit dieser Methode hochrealistische, frei navigierbare Rekonstruktionen erzeugen lassen, selbst wenn nur begrenztes Ausgangsmaterial vorhanden ist (Malik et al., 2024). Damit eröffnet sich insbesondere für die nachträgliche Rekonstruktion von dynamischen Ereignissen – etwa bei Überwachungsvideos – ein neues Anwendungsfeld. Gleichzeitig stellt sich die Frage nach Validierbarkeit, Manipulationssicherheit und gerichtlicher Zulässigkeit solcher KI-generierten Szenenmodelle.

Während sich ein Großteil der Forschung auf visuelle und räumliche Rekonstruktion konzentriert, erweitert die forensische Chemie das Spektrum der Tatortanalyse auf molekularer Ebene. Logrado (2025) beschreibt in einer Übersicht zur Kohlenwasserstoff-Forensik die Bedeutung chemischer Signaturanalysen für Branddelikte, Umweltkriminalität oder Treibstoffmanipulation. Moderne analytische Verfahren erlauben die differenzierte Identifikation von Herkunft, Zusammensetzung und Transformationsprozessen chemischer Substanzen (Logrado, 2025). Damit zeigt sich, dass Tatortrekonstruktion nicht ausschließlich visuell oder digital zu verstehen ist, sondern weiterhin tief in naturwissenschaftlicher Analytik verwurzelt bleibt. Vielmehr entsteht ein hybrides Modell, in dem chemische, physikalische und digitale Datensätze integriert werden (Bergmann et al., 2024).

In der Zusammenschau der genannten Arbeiten wird deutlich, dass sich Crime Scene Reconstruction zu einem integrativen Forschungsfeld entwickelt, das drei zentrale Entwicklungslinien vereint: Erstens die Standardisierung und Methodisierung des Rekonstruktionsprozesses (Balbudhe et al., 2025), zweitens die Digitalisierung und dreidimensionale Modellierung des Tatortes (Carew et al., 2021; Bostanci, 2015) und drittens die KI-gestützte, immersive Erweiterung durch Deep Learning und Extended Reality (Zappalà et al., 2024; Malik et al., 2024; Chango, 2025).

Diese Entwicklung hat weitreichende epistemologische Konsequenzen. Der Tatort ist nicht mehr nur physischer Raum, sondern wird zu einem datengenerierenden System, das in unterschiedlichen Modalitäten – visuell, chemisch, digital – repräsentiert werden kann. Rekonstruktion bedeutet somit nicht mehr allein retrospektive Narration, sondern modellbasierte Simulation und probabilistische Bewertung. Gleichzeitig bleibt die Frage der Validierung zentral: Je stärker Rekonstruktionen algorithmisch erzeugt oder KI-gestützt optimiert werden, desto dringlicher wird die Forderung nach Transparenz, Nachvollziehbarkeit und gerichtsfester Dokumentation.

Abb. 2: Überblick über Techniken (KI-generiert): A Digitale Spiegelreflexkamera bei der Tatortaufnahme, B UV-Forensikkamera macht Blutspuren sichtbar, C Wärmebildkamera im nächtlichen Einsatz, D 3D-Tatortscan (Innenraum), E Drohne zur Unfallaufnahme aus der Luft

Die aktuelle Forschung verdeutlicht daher eine doppelte Bewegung: Einerseits wächst die technologische Komplexität der Tatortrekonstruktion durch 3D-Scanning, KI, NeRF und Extended Reality erheblich. Andererseits besteht ein zunehmender Bedarf an methodischer Rahmung, Standardisierung und interdisziplinärer Qualitätssicherung. Crime Scene Reconstruction im 21. Jahrhundert ist somit weder rein kriminalistisch noch rein technologisch, sondern ein transdisziplinäres Feld, das naturwissenschaftliche Präzision, digitale Innovation und kriminalistische Logik miteinander verbinden muss.

Die skizzierte Entwicklung macht deutlich, dass die technologische Erweiterung der Tatortrekonstruktion nicht bei der dreidimensionalen Modellierung oder immersiven Visualisierung endet. Vielmehr entsteht aus der Kombination standardisierter Rekonstruktionsmethoden, hochauflösender 3D-Erfassung und KI-gestützter Analyse eine neue Qualität digitaler Tatortrepräsentation. Während einzelne Technologien – etwa Laserscanning, Photogrammetrie oder Deep Learning – jeweils spezifische Funktionen erfüllen, eröffnet erst ihre systematische Integration die Möglichkeit, Tatorte als konsistente, langfristig nutzbare und interaktiv analysierbare Datenräume zu verstehen.

Damit verschiebt sich der Fokus von der punktuellen Rekonstruktion einzelner Ereignisabläufe hin zur Schaffung eines persistenten digitalen Referenzmodells, das unterschiedliche Datentypen – geometrische, visuelle, chemische und algorithmisch generierte Informationen – in einer gemeinsamen Struktur zusammenführt. Diese Integrationsleistung bildet die konzeptionelle Grundlage dessen, was in der forensischen Praxis zunehmend als „digitaler Zwilling“ bezeichnet wird. Der digitale Zwilling ist somit nicht lediglich eine Weiterentwicklung der 3D-Modellierung, sondern die strukturelle Verdichtung der zuvor beschriebenen technologischen Entwicklungslinien. Vor diesem Hintergrund ist die Bedeutung des forensischen digitalen Zwillings für die moderne Polizeitechnik nicht als isolierte Innovation zu verstehen, sondern als logische Konsequenz der fortschreitenden Digitalisierung, Standardisierung und Simulation kriminalistischer Prozesse.

Bedeutung des forensischen digitalen Zwillings für die moderne Polizeitechnik

Der Begriff des „digitalen Zwillings“ wurde in der forensischen Praxis nicht abrupt eingeführt, sondern entwickelte sich schrittweise aus bereits bestehenden digitalen Dokumentations- und Rekonstruktionsverfahren. In der Vorläuferphase zwischen etwa 1995 und 2010 existierte der digitale Zwilling noch nicht als expliziter Terminus, wohl aber als implizites Konzept. In dieser Zeit entstanden digitale Tatortfotografien, CAD-basierte Rekonstruktionen, erste dreidimensionale Modelle auf Grundlage von Messdaten sowie virtuelle Unfallrekonstruktionen. Die Fachsprache sprach damals von „virtueller Rekonstruktion“, „3D-Tatortmodell“ oder „digitaler Tatortabbildung“. Gleichwohl handelte es sich noch nicht um digitale Zwillinge im engeren Sinne, da die Modelle meist nur Teilbereiche erfassten, keine vollständig konsistente Geometrie aufwiesen und keine dauerhafte, systematisch integrierte Datenbasis boten.

Eine Übergangsphase lässt sich etwa zwischen 2010 und 2015 verorten. Mit dem breiten Einsatz von 3D-Laserscannern, photogrammetrischen Verfahren, 360°-Kameras und Drohnenaufnahmen wurden erstmals vollständige, messbare 1:1-Abbilder von Tatorten möglich. Die forensische Praxis begann zunehmend von „virtuellen Tatorten“, „digitalen Tatorten“ oder

„3D-Tatortabbildern“ zu sprechen. Während der Begriff „digitaler Zwilling“ in der Industrie – insbesondere im Kontext von Industrie 4.0 – bereits etabliert war, wurde er im forensischen Bereich noch zurückhaltend verwendet. Die technischen Voraussetzungen für ein maßstabsgetreues digitales Abbild waren nun zwar weitgehend gegeben, doch fehlte noch die klare begriffliche Einordnung.

Erst ab etwa 2016 bis 2018 lässt sich eine explizite Übernahme des Begriffs „digitaler Zwilling“ in den forensischen Diskurs beobachten. In wissenschaftlichen Publikationen, Fachvorträgen, Schulungen sowie bei der Präsentation komplexer Rekonstruktionsmodelle vor Gericht wurde der Terminus zunehmend verwendet. Dieser Zeitpunkt ist kein Zufall: Jetzt waren vollständige 3D-Erfassungen möglich, die sowohl präzise Geometrie als auch realitätsnahe Textur integrierten. Die Modelle erlaubten reproduzierbare Messungen, langfristige digitale Speicherung, virtuelle Begehungen sowie nachträgliche Analysen unabhängig vom realen Tatort. Damit erfüllten digitale Tatortabbilder erstmals die zentralen Kriterien eines digitalen Zwillings: Maßstabsgenauigkeit, Vollständigkeit, Konsistenz und nachhaltige Nutzbarkeit.

Seit etwa 2020 ist der Begriff im forensischen Fachkontext weitgehend akzeptiert, wenngleich er bewusst und präzise verwendet wird. In der Forensik bezeichnet der digitale Zwilling ein maßstabsgetreues, unveränderliches digitales Abbild eines realen Tatortes oder Beweisobjektes, das Analyse, Rekonstruktion, Hypothesenprüfung und Präsentation ermöglicht. Typische Anwendungsfelder sind die Tatort- und Unfallrekonstruktion, die Hypothesenprüfung, der Vergleich alternativer Szenarien, die Ausbildung und Schulung von Einsatzkräften sowie die anschauliche Darstellung und Präsentation komplexer Sachverhalte im Gerichtsverfahren.

Heute stellt der digitale Zwilling einen integralen Bestandteil moderner Polizeitechnik dar. Er ermöglicht eine Trennung zwischen realem Tatort und Analyseumgebung, wodurch Beweise geschont und dennoch umfassend ausgewertet werden können. Zudem erlaubt der digitale Zwilling eine interdisziplinäre Zusammenarbeit zwischen Kriminaltechnik, Rechtsmedizin, Unfallanalyse und Justiz.

Gleichzeitig stellt der Einsatz digitaler Zwillinge hohe Anforderungen an Datenintegrität, Dokumentation und Nachvollziehbarkeit, um gerichtsfest zu bleiben. Gerade die Darstellung komplexer Sachverhalte vor Gericht geht mit Herausforderungen einher. Der Beitrag von A. Holzer et al., 2025, zeigt, welche „Gefahren“ sich bei der Bildgebung mittels 3D-Technik aus strafprozessualer Hinsicht ergeben können und wie vor dem Hintergrund der freien richterlichen Beweiswürdigung der Spagat zwischen Visualisieren und Suggerieren gelingen kann.

Die strafprozessuale Einordnung dreidimensionaler Visualisierungen verdeutlicht, dass der digitale Zwilling nicht nur eine technische Innovation, sondern zugleich ein normativ sensibles Instrument darstellt. Die Frage, inwieweit Visualisierungen lediglich veranschaulichen oder bereits interpretativ strukturieren, berührt den Kern der freien richterlichen Beweiswürdigung. Digitale Modelle können komplexe Sachverhalte transparent machen, sie können jedoch – bewusst oder unbewusst – auch suggestive Wirkungen entfalten. Damit verschiebt sich die Verantwortung von der rein technischen Präzision hin zur methodischen Transparenz und dokumentierten Nachvollziehbarkeit der Modellierungsschritte.

Gerade diese Ambivalenz macht deutlich, dass der forensische digitale Zwilling nicht isoliert als Visualisierungswerkzeug verstanden werden darf. Seine eigentliche Bedeutung entfaltet sich erst im Kontext eines strukturierten, hypothesengeleiteten Erkenntnissystems, in dem Modellierung, Simulation und Beweisverknüpfung methodisch kontrolliert erfolgen. Der digitale Zwilling ist somit nicht nur Präsentationsmedium, sondern integraler Bestandteil eines erweiterten kriminalistischen Analyseprozesses. Vor diesem Hintergrund gewinnt das Konzept des Forensiums besondere Relevanz: Es beschreibt den Übergang vom digitalen Tatortabbild hin zu einem gekoppelten Simulations- und Erkenntnissystem, das Rekonstruktion, Hypothesenprüfung und interdisziplinäre Zusammenarbeit in einer kohärenten Architektur zusammenführt.

Der forensische digitale Zwilling in der Tatortrekonstruktion und Hypothesenprüfung – Forensium

Die fortschreitende Digitalisierung forensischer Arbeitsprozesse markiert keinen bloßen technologischen Fortschritt, sondern eine tiefgreifende epistemische Transformation kriminalistischer Erkenntnis. Während die klassische Tatortarbeit über Jahrzehnte primär dokumentationsbasiert organisiert war, etabliert sich mit dem digitalen Zwilling eine neue Form der persistenten, modellbasierten Analyse (Labudde, 2026). Das Forensium bezeichnet in diesem Zusammenhang eine systematische Erweiterung des digitalen Zwillings zu einem gekoppelten Erkenntnissystem, das dreidimensionale Raumrepräsentation, strukturierte Evidenzobjekte, agentenbasierte Simulation und intelligente Datenverarbeitung in einer integrativen Architektur vereint (Labudde, 2026).

Diese Entwicklung ist zugleich eingebettet in eine breitere wissenschaftliche Bewegung hin zu simulationsbasierten Erkenntnismodellen komplexer Systeme, wie sie insbesondere in der Urbanistik und Komplexitätsforschung ausgearbeitet wurden (Batty, 2013; Portugali, 2011).

Historisch ist die forensische Dokumentation eng mit der Entwicklung der Tatortfotografie verbunden. Ziel war stets die objektive, vollständige und maßstabsgetreue Erfassung eines Zustandes. Fotografien, Skizzen und Vermessungsdaten dienten der Konservierung eines Tatortes, der sich im Zuge der Ermittlungen zwangsläufig veränderte. Diese Arbeitsweise ist strukturell destruktiv: Mit jeder Spurensicherung wird die ursprüngliche Konstellation modifiziert, räumliche Relationen werden aufgelöst und müssen später rekonstruiert werden. Die Integration einzelner Beweise in ein kohärentes Gesamtbild bleibt interpretativ und ist kognitiven Verzerrungen zugänglich. Der digitale Zwilling transformiert diesen Prozess grundlegend (Labudde, 2026). Durch 3D-Laserscanning, Photogrammetrie, 360°-Erfassung und multimodale Datensammlung entsteht ein persistenter, maßstabsgetreuer digitaler Raum, der unabhängig vom physischen Tatort analysierbar bleibt. Dieser Raum ist nicht nur visuelle Repräsentation, sondern eine strukturierte Datenumgebung. Geometrische Informationen werden mit semantischen Attributen verknüpft und bilden eine Grundlage für weiterführende Analysen. In struktureller Hinsicht entspricht diese Raumkonzeption digitalen Geosimulationsmodellen, wie sie in der räumlichen Modellierung urbaner Prozesse entwickelt wurden (Benenson & Torrens, 2004). Der Tatort wird damit als diskreter oder kontinuierlicher Zustandsraum modelliert, dessen Dynamik formal beschrieben werden kann.

Die strukturelle Logik dieser Transformation wird in Abbildung 3 verdeutlicht (vgl. Labudde, 2026, Abb. 1). Dort ist die schrittweise Überführung des physischen Tatortes in einen erweiterten virtuellen Raum dargestellt. Zunächst wird ein digitaler Tatort erzeugt, der sämtliche Objekte einschließlich potenzieller Beweisträger umfasst. Relevante Beweisstücke werden physisch ins Labor überführt, analysiert und anschließend als strukturierte Daten wieder in das digitale Modell integriert. Durch diese kontinuierliche Anreicherung entsteht ein „extended virtual crime scene", der als Grundlage für die Verifikation und Falsifikation kriminalistischer Hypothesen dient (Labudde, 2026).

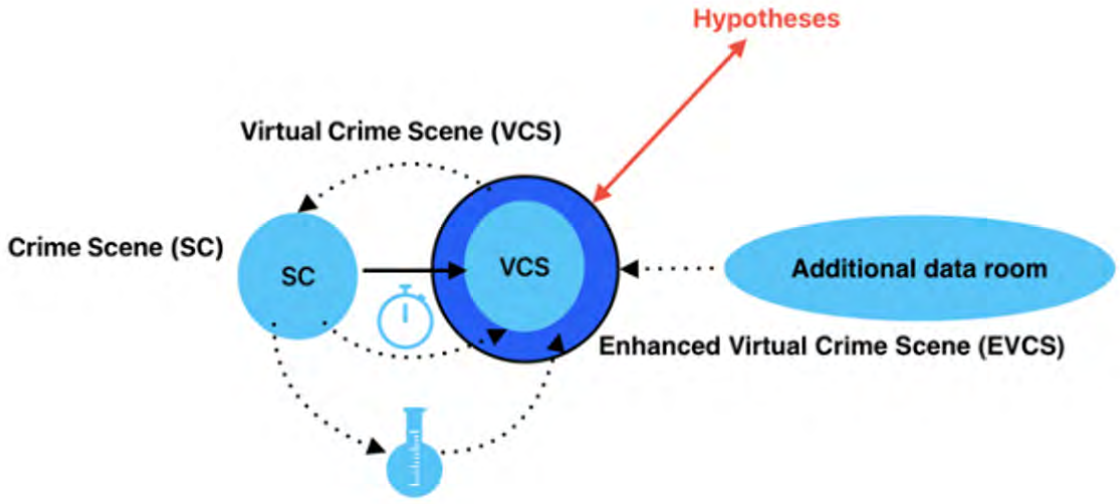


Abb. 3: Vom physischen Tatort zum erweiterten digitalen Zwilling (nach Labudde, 2026). Darstellung der Transformation eines realen Tatortes in ein virtuelles 3D-Modell, das durch Laboranalysen und zusätzliche Dateneinbindung zu einem erweiterten, hypothesenfähigen Rekonstruktionsraum angereichert wird.

Eine zentrale Voraussetzung hierfür ist die Neubestimmung des Beweismittels. Im Forensium wird Evidenz nicht mehr primär als Objekt verstanden, sondern als informationslogische Einheit mit räumlich-zeitlicher Einbettung (Labudde, 2026). Formal lässt sich ein Beweis als Funktion von Raum- und Zeitparametern beschreiben (Labudde, 2026). Diese Abstraktion entspricht der Modelllogik komplexer Systeme, in denen Mikroinformationen makroskopische Muster erzeugen (Portugali, 2011).

Ontologisch wird jedes Beweisstück durch eine dreistufige Struktur erfasst: Objekt, Attribut, Wert (vgl. Labudde, 2026). Diese Strukturierung erlaubt maschinelle Verarbeitung, semantische Verknüpfung und simulationsbasierte Hypothesenprüfung. Der digitale Tatort wird damit zu einem relationalen Informationsnetzwerk. Für das Verständnis des Forensiums ist die Unterscheidung zwischen digitaler Kopie und digitalem Zwilling entscheidend (Labudde, 2026). Während die digitale Kopie statisch bleibt, ist der digitale Zwilling dynamisch, multimodal und zeitübergreifend erweiterbar. Diese Dynamisierung entspricht der Logik komplexer adaptiver Systeme, deren Zustand nicht isoliert, sondern prozessual verstanden werden muss (Batty, 2013).

Der eigentliche Innovationsschritt liegt in der Erweiterung dieses digitalen Zwillings zum Forensium als gekoppeltem System (Labudde, 2026). Die Architektur des Forensiums wird in Abbildung 4 dargestellt (nach Labudde, 2026, Abb. 2). Analog zu hybriden Modellen aus

zellulären Automaten und agentenbasierten Simulationen (Portugali, 2000) bewegen sich autonome Akteure innerhalb eines dreidimensionalen Raumes. Diese Kopplung entspricht dem FACS-Modell (Free Agents in a Cellular Space), das die räumliche Logik zellulärer Automaten mit der Entscheidungslogik autonomer Agenten verbindet (Portugali, 2000). Vergleichbare Modellierungsansätze finden sich in der Geosimulation urbaner Phänomene (Benenson & Torrens, 2004).

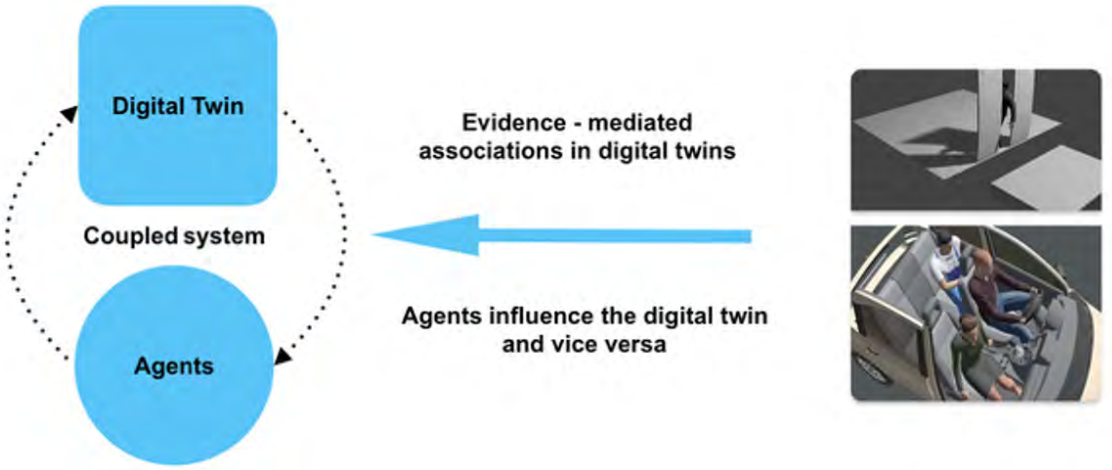


Abb. 4: Das Forensium als gekoppeltes System (nach Labudde, 2026). Schematische Darstellung der Kopplung eines digitalen 3D-Tatortmodells mit agentenbasierten Simulationen (FRE3 – Free Agents in 3D Environment).

Analoge und digitale Beweise vermitteln zwischen Raumstruktur und simulierten Akteuren; Physik-Engines ermöglichen realitätsnahe Interaktionen.

Die Kopplung erfolgt über Beweise und Informationsflüsse (Labudde, 2026). Physik-Engines berechnen Bewegungen, Kollisionen, Sichtlinien oder Sturzszenarien. Rekonstruktion wird dadurch zu einem experimentellen Verfahren im Sinne simulationsbasierter Hypothesenprüfung. Die Einbindung subjektiver Zeugenaussagen erweitert diese Struktur um eine epistemologische Dimension. Large Language Models ermöglichen die Strukturierung unstrukturierter Aussagen und deren Integration in den digitalen Raum (Labudde, 2026). Die Analyse verschiebt sich damit von narrativer Plausibilität zu physikalischer Möglichkeit (Volkmann et al., 2025).

Der Paradigmenwechsel ist deutlich: Klassische Beweissicherung ist dokumentations- und interpretionsbasiert. Das Forensium etabliert einen konservativen, simulationsbasierten Ansatz. Der Tatort bleibt als persistenter, interaktiver Datenraum erhalten. Hypothesen können experimentell geprüft und alternative Szenarien modellbasiert verglichen werden. In systemtheoretischer Perspektive lässt sich das Forensium als Anwendung komplexitätswissenschaftlicher Modellierungslogiken auf die Forensik verstehen (Batty, 2013; Portugali, 2011).

Referenzen

Balbudhe, M. S., Shetty, B. S. K., Kumar, N. A., Singh, D., & Sherekar, A. I. (2025). Crime scene reconstruction: A scoping review. *Egyptian Journal of Forensic Sciences*, 15, 79. https://doi.org/10.1186/s41935-025-00495-5

Batty, M. (2013). *The new science of cities*. MIT Press.

Benenson, I., & Torrens, P. M. (2004). *Geosimulation: Automata-based modeling of urban phenomena.* Wiley.

Bertillon, A. (1890). *La photographie judiciaire: Avec un appendice sur la classification et l'identification anthropométriques*. Gauthier-Villars.

Bergmann, T., Bodach, R., Pistorius, L., Preuß, S., Seidel, P., & Labudde, D. (2024). Colors in forensics: The analysis and visualization of forensic data and evidence. In *Dye chemistry: Exploring colour from nature to lab*. IntechOpen. https://doi.org/10.5772/intechopen.1006108

Bostanci, E. (2015). *3D reconstruction of crime scenes and design considerations*. arXiv. https://doi.org/10.48550/arXiv.1512.03156

Carew, R. M., Morgan, B., & Rando, C. (2021). 3D forensic science: A new field integrating 3D imaging and analysis. *Forensic Science International: Synergy, 3*, 100205. https://doi.org/10.1016/j.fsisyn.2021.100205

Chango, X., Flor-Unda, O., Bustos-Estrella, A., Gil-Jiménez, P., & Gómez-Moreno, H. (2025). Extended Reality Technologies: Transforming the Future of Crime Scene Investigation. *Technologies*, *13*(8), 315. https://doi.org/10.3390/technologies13080315

de Castro, A., Andenaes, K., & Larsen, R. (2018). Multispectral imaging in forensic science: A review. *Journal of Forensic Radiology and Imaging, 15*, 1–9.

Edelman, G., van Leeuwen, T. G., & Aalders, M. C. (2012). Hyperspectral imaging for non-contact analysis of forensic traces. *Forensic Science International, 223*(1–3), 28–39. https://doi.org/10.1016/j.forsciint.2012.08.003

Gardner, R. M., & Krouskup, D. R. (2018). *Practical crime scene processing and investigation*. CRC Press.

Gross, H. (1893). *Handbuch für Untersuchungsrichter als System der Kriminalistik*. F. C. W. Vogel.

Holzer, A., Cornelius, K., & Labudde, D. (2025). Die „Gefahren" der Verwendung von 3D-Techniken im Strafverfahren. *Kriminalistik*, März-Ausgabe 2025.

Labudde, D. (2026). Forensium – The digital twin in forensic casework. In *Proceedings of the conference* (pp. 1–5). IARIA.

Lograd, L. P. L. (2025). Hydrocarbon forensic chemistry: Exploring multiple fronts – a mini-review. *Forensic Sciences Research.* https://doi.org/10.1093/fsr/owaf047

Malik, S. N., Chee, M. H., Perera, D. M. A., & Lim, C. H. (2024). *Feasibility of neural radiance fields for crime scene video reconstruction.* arXiv https://doi.org/10.48550/arXiv.2407.08795

Nafte, M. (2009). *Crime scene photography*. Academic Press.

Portugali, J. (2000). Self-organization and the city. In *Self-organization and the city* (Chap. 5, "Free agents in a cellular space"). Springer. https://doi.org/10.1007/978-3-662-04099-7_5

Portugali, J. (2011). *Complexity, cognition and the city.* Springer.

Richards, A. L., & Siebert, J. P. (2017). LiDAR and structured light scanning for forensic documentation. *Journal of Forensic Sciences, 62*(6), 1585–1593.

Robinson, E. M. (2010). *Crime scene photography*. Academic Press.

Saferstein, R. (2020). *Criminalistics: An introduction to forensic science*. Pearson.

Thali, M. J., Braun, M., & Dirnhofer, R. (2003). Optical 3D surface digitizing in forensic medicine: 3D documentation of skin and bone injuries. *Forensic Science International*, 137(2–3), 203–208.

Urbanová, P., Hejna, P., Jurda, M., & Krajsa, J. (2015). Photogrammetry in forensic practice: A comprehensive review. Forensic Science International, 250, 77–89. https://doi.org/10.1016/j.forsciint.2015.02.028

Volkmann, D., Schildein, S., Povalej, R., & Labudde, D. (2025). A case study for immersive technology-based evidence representation. Springer. https://link.springer.com/book/10.1007/978-3-032-07986-2

Zappalà, A., Guarnera, L., Rinaldi, V., Livatino, S., & Battiato, S. (2024). Enhancing crime scene investigations through virtual reality and deep learning techniques. arXiv. https://doi.org/10.48550/arXiv.2409.18458

Von MS Paint bis Deepfakes – Digitale Fälschungen seit 2000 als Herausforderung für Polizei und Forensik

Robert Diedrich Ulrich Lippitz

Abb. 1: Die Hinrichtung der ‚Geiseln der Kommune' vor ihrer Exekution am Gefängnis La Grande Roquette, Eugène Appert, 24.05.1871

Es ist Ende Mai 1871 in Paris. Während der Rückeroberung durch die Versailler Truppen eskaliert der Bürgerkrieg in der französischen Hauptstadt. In der Haftanstalt La Grande Roquette erschießen die Mitglieder der Kommune den Pariser Erzbischof und weitere Mönche. Fotograf Eugène Appert hält die Exekution sowie weitere Gewaltakte der sog. Blutwoche fest (Vormweg, 2021).

Doch die vermeintliche Evidenz trügt: Die Fotoreihe ist eine Fälschung. Appert stellte sie aus Aufnahmen mit Statisten her, montierte die Szenen in passende Hintergründe und tauschte die Gesichter mit Aufnahmen, die er von den Mönchen und dem Erzbischof im Gefängnis geschossen hatte. Es ging nicht um die Dokumentation eines realen Ereignisses, sondern um politische Inszenierung (von Lüpke, 2014). Dies zeigt damit schon zum frühest denkbaren Zeitpunkt: Die Geschichte fotografischer Fälschung beginnt nicht erst im digitalen Zeitalter, sondern nahezu zeitgleich mit der Erfindung der Fotografie selbst.

Doch auch schon lange vor Fotografie, Computer und Künstlicher Intelligenz wurden Fälschungen zur politischen Inszenierung angefertigt. Schon 1247 v. Chr. ließ Pharao Ramses II. Gedichte verfassen und Bildnisse eines großen Sieges in einer Schlacht meißeln, die er

eigentlich verloren hatte (Herzog, 2024), und 335 v. Chr. schlug Alexander der Große einen Aufstand in Theben nieder, der entstanden war, nachdem antike Fake-News fälschlicherweise die Geschichte seines Todes verbreitet hatten (Lamm, 2025).

Fälschung, Täuschung und Inszenierung sind folglich keine Produkte der Moderne, sondern Konstanten der Menschheitsgeschichte. Sie werden nicht nur für politische Zwecke genutzt. Alles, was von Wert ist, kann und wird durch kriminelle Strukturen gefälscht werden: Von unechten Kunstwerken und Geld über die Fälschung von Medikamenten, Elektrogeräten und Spielzeug bis hin zu dem „großen Weinschwindel“ (Steck, 2007) – den Modi Operandi sind keine Grenzen gesetzt.

Digitale Fälschungen in der Moderne

Insbesondere im digitalen Raum sind Fälschungen von Bedeutung, da sie sich mit geringem Aufwand herstellen, vervielfältigen und verbreiten lassen. Dabei können nicht nur Inhalte gefälscht, sondern vollständige künstliche Identitäten aufgebaut und glaubhaft aufrechterhalten werden. Zugleich ist ihr Nachweis erschwert, weil Manipulationen technisch leicht verschleiert und Inhalte schnell weiterverbreitet werden.

Seit dem Jahr 2000 hat die Digitalisierung das polizeiliche und gerichtliche Beweisverfahren grundlegend verändert. Aus der zunehmenden Verlagerung des Alltags ins Internet folgt eine gestiegene Bedeutung digitaler Beweismittel (Momsen & Hercher, 2014). Traditionell dienten technische Mittel wie die Fotografie der Objektivierung der Realität, sodass Lichtbilder vor Gericht als verlässliches Beweismittel hohe Anerkennung genießen (Rabe, 2020). Mit dem Voranschreiten der Technik wächst jedoch gleichermaßen die Möglichkeit zur Manipulation der Beweise. Die Polizeitechnik steht seit jeher vor der Aufgabe, die Authentizität digitaler Beweismittel sicherzustellen, was insbesondere durch neuere Entwicklungen in der KI-Technologie zunehmend erschwert wird.

Dieser Beitrag soll aufzeigen, wie das Prinzip der Fälschung durch gesteigerte Geschwindigkeit, Skalierbarkeit und Verfügbarkeit eine neue Qualität annimmt, die über die bloße Manipulation einzelner Inhalte hi-nausgeht und die Konstruktion von Realität insgesamt berührt.

Zur Aufarbeitung der Fälschungshistorie und polizeilicher Reaktionen wird die Entwicklung digitaler Manipulationstechnologien in drei Perioden unterteilt und anhand zeitgenössischer Quellen analysiert: angefangen mit der Phase der Desktop-Manipulation und klassischer Bildforensik (ca. 2000 – ca. 2010), in der die Manipulation vor allem ein handwerkliches Problem war, über die Phase der Plattformisierung und Skalierung (ca. 2010 – ca. 2017), in der besonders die allgegenwärtige Nutzung von sozialen Netzwerken und mobilen Endgeräten den digitalen Raum mit digitalen Inhalten flutete. Die dritte Phase der KI-Synthese (seit ca. 2017) wird durch Deepfakes repräsentiert, die durch Qualität, Simplizität und Automatisierbarkeit einen Paradigmenwechsel in der Generierung von gefälschten Inhalten einleiteten. Abschießend sollen polizeiliche Reaktionsstrategien vorgeschlagen sowie ein Ausblick auf zukünftige Entwicklungen gegeben werden.

Phase 1 – Photoshop und Desktop-Manipulation

Die Geschichte der Bildfälschung fängt wie beschrieben weit vor der Möglichkeit der digitalen Manipulation an, was an zahlreichen Beispielen belegt ist: Stalin ließ politische Gegner wie Leo Trotzki oder Nikolai Jeschow aus Fotos herausretuschieren, indem die Negative übermalt oder Personen weggekratzt wurden. Hintergründe und entstandene Lücken wurden mit Treppen, Mauern, Menschenmengen oder anderen Bildteilen aufgefüllt, um die Manipulation zu verschleiern (Waschik, 2010). Auch eins der bekanntesten Bilder von Abraham Lincoln basiert auf einem Gemälde, das John C. Calhoun abbildet, auf das eine Fotografie von Lincolns Gesicht gespiegelt und montiert wurde, bevor die Montage in den Druck ging (Macdonald, 2024). Die Bildmanipulation ist zu diesem Zeitpunkt von schwierigen handwerklichen Arbeiten, spezialisierten Werkzeugen und erheblicher Fachexpertise geprägt.

Abb. 2: Links Originalportrait John C. Calhouns, rechts Fotomontage von Abraham Lincoln. BBC Culture, nach Macdonald (2024).

Desktopmanipulation in den 2000ern: Alte Logik, neue Werkzeuge

In den 2000er Jahren werden digitale Fälschungen insbesondere durch die inzwischen weit verbreitete Digitalfotografie bestimmt. Die Schwierigkeiten bei digitalen Fälschungen verändern sich dadurch grundlegend, die Herangehensweise bleibt aber aufwendig: Die handwerkliche Arbeit besteht nun vor allem im digitalen Klonen, Retuschieren und Zeichnen; die speziellen Werkzeuge finden sich in komplexen Programmen, deren Bedienung weiterhin anspruchsvoll ist. Die hierfür erforderliche Expertise musste in der Regel nach wie vor gezielt, etwa durch Fachliteratur oder Kurse, erworben werden (Bredenfeld, 2008).

Das prägendste Werkzeug in der Fotomanipulation ist seit jeher das Adobe Programm Photoshop. Das Wort „photoshoppen“ wurde im öffentlichen Diskurs geradezu zum Synonym für Fotomanipulation und in den 2000er Jahren sogar in den Duden aufgenommen. Schon zu diesem Zeitpunkt waren die verfügbaren Funktionen umfassend und insbesondere die

Einführung des Verflüssigungsfilters (2000) sowie des Bereichsreparaturpinsels, der Verzerrungsfunktion, Schnellauswahlwerkzeuge und Smart-Objekte (2005) erhöhten die Qualität und die Benutzungsfreundlichkeit zunehmend (Pearce, 2008).

Insbesondere fünf Funktionsgruppen, die zu diesem Zeitpunkt schon problemlos nutzbar waren, sind für die Fotomanipulation entscheidend:

- *Ebenen*, *Auswahlen* und *Masken*, weil damit Bildteile getrennt, verdeckt, freigestellt und neu zusammengesetzt werden konnten.
- *Kopierstempel*, *Reparatur-Pinsel* und *Ausbessern-Werkzeug*, also Werkzeuge zum Kopieren, Retuschieren und unauffälligem Ersetzen von Bildbereichen.
- *Transformieren-* bzw. *Verkrümmen-Funktionen* und später *Fluchtpunkt*, weil sich damit Perspektive, Größe und Form angepasster Elemente glaubwürdig angleichen ließen.
- Farb- und Tonwertkorrekturen wie *Einstellungsebenen* und *Gleiche Farbe*, um montierte Bildteile optisch an den Kontext anzupassen.
- Hilfsmittel wie Weichzeichner oder künstliches Rauschen – etwa über *Rauschen hinzufügen* –, mit denen Übergänge, Schärfe und Oberflächenstruktur homogener gemacht werden konnten.

Die kriminalistische Bedeutung liegt also nicht in einer einzelnen Fälschungsfunktion, sondern in einer Kombination aus Ebenen-Technik, präziser Retusche, perspektivischer Anpassung und unauffälliger Farbangleichung.

Einer der ersten prominenten Fälle, in dem eine solche Technik auffiel, war der Reuters-Fall von 2006: Der Fotograf Adnan Hajj verbreitete eine Aufnahme aus Beirut, bei der der aufsteigende Rauch verändert worden war, um die Zerstörung nach dem israelischen Angriff zu dramatisieren. Deutlich zu erkennen ist der Einsatz des Kopierstempels – anhand der teils mitkopierten Häuserfassaden und der sich exakt wiederholenden Pixelmuster – sowie der Nachdunkeln-Funktion. Nach Bekanntwerden der Manipulation zog Reuters das Bild zurück, beendete die Zusammenarbeit mit Hajj und verschärfte in der Folge seine internen Regeln für die Bildbearbeitung erheblich (Reuters, 2007).

Abb. 3: „Smoke billows from burning buildings destroyed during an overnight Israeli air raid on Beirut's suburbs", Adnan Hajj, Bronxdoc.org, 05.08.2006. Original links, bearbeitete Fassung rechts, Gegenüberstellung durch Autor.

Die Anwendung von Photoshop in der breiten Masse der Delinquenten wurde seit jeher wohl aufgrund des hohen Preises gebremst (Preis Version 1 1990 betrug 895 $, inflationsbereinigt über 2000 $). GIMP, das funktional eine mit Photoshop vergleichbare Produktpalette bereitstellt, ist seit 1996 vollständig kostenfrei verfügbar und entwickelte sich insbesondere seit der Veröffentlichung von Version 2.0 im Jahr 2004 auch außerhalb der Linux-Welt zur maßgeblichen Mainstream-Alternative zu Adobes marktführendem Produkt (Gilbertson, 2008; GIMP, o. J.).

Dies bedeutete jedoch nicht, dass digitale Fälschungen in dieser Phase ausschließlich mit hochtechnologischen Mitteln erstellt wurden, da insbesondere die Einstiegshürde im Vergleich zur analogen Fälschung deutlich abgesenkt wurde, was bspw. ein Fall aus Irland zeigt: Der Finanzanalyst Neil Dolan nutzte das bei Windows vorinstallierte Programm MS Paint, um Identitätsdokumente zu fälschen und unter falschem Namen Kreditanträge zu stellen (Ferguson, 2018).

GIMP, Paint, Photoshop und andere Programme unterschieden sich zwar in ihrer Anwendung, nicht jedoch in ihrer grundlegenden Funktionsweise: Mit ihnen war es lediglich möglich, Bilder zu bearbeiten, nicht aber, sie zu synthetisieren, was für die Polizei einen entscheidenden Vorteil darstellte. Die Fotomontagen hinterließen in den Dateien Spuren, auf die die Forensik bald aufmerksam wurde.

Forensische Antwort: Vom Lichtbild zum Spurenträger

Die polizeitechnische Reaktion auf diese digitalen Bildfälschungen war im Kern, dass Lichtbilder nicht mehr allein als sichtbare Abbildung, sondern zugleich als technische Spurenträger behandelt wurden. Die Untersuchung verlagerte sich von dem rein Sichtbaren zunehmend auf die Ebene der Dateistruktur, der Pixelstatistiken und der gerätespezifischen Entstehungsspuren (Böhme et al., 2009; Kirchner 2006). Während bei analogen Bildfälschungen besonders das Material technisch im Labor untersucht wurde, rückten nun digitale Verfahren in den Vordergrund, die nach statistischen oder physikalischen Inkonsistenzen suchten, die beim Erstellen und Bearbeiten von Bildern entstehen.

Dieser Perspektivwechsel schlug sich in neuen forensischen Methoden nieder, die unter anderem folgende Spuren ermitteln konnten:

- *Copy-Move-Artefakte*: Spuren, die entstehen, wenn Bildteile aus demselben Foto kopiert und an einer anderen Stelle wieder eingefügt werden. Auch wenn diese Manipulationen visuell unauffällig sind, sind die mathematischen Bildwerte auffällig, weil sie identisch oder zumindest stark korrelierend sind (Popescu & Farid, 2004; Farid, 2009).
- *Re-Sampling-Artefakte*: Sie entstehen durch geometrische Transformationen, also etwa durch Skalierung, Rotation oder perspektivische Anpassung von Bildteilen, und zeigen sich in periodischer Korrelation benachbarter Pixel (Kirchner, 2006).
- *Sensorrauschen*: Die verbauten lichtempfindlichen Sensoren von Kameras hinterlassen aufgrund minimaler Fertigungsabweichungen ein individuelles Rauschen, das eine Art „Fingerabdruck der Kamera“ (Dreschler-Fischer & Spitzer, 2009, S. 56)

darstellt. Schon im Jahr 2006 konnten Lukás et al. Aufnahmen konkreten Kameras zuordnen, und Kirchner betont, dass dies sogar nach Kompression des Bildes noch möglich war (Lukás et al., 2006; Kirchner 2006).

- *Verzerrungen* und *Filter*: Die auf die Originaldatei angewendeten Veränderungen funktionieren nach einem nachvollziehbaren mathematischen Algorithmus, der, wenn er bekannt ist, zurückgerechnet werden kann. Ein eindrucksvolles Beispiel ist die Operation VICO. INTERPOL fahndete dabei mit einer Fotografie eines pädokriminellen Täters, der aufgrund der auf das Gesicht angewandten Verzerrung unter dem Namen „Swirl Face" bekannt wurde. Digitalforensiker des BKA konnten die Verzerrung technisch zurückrechnen und so ein wiedererkennbares Fahndungsbild erzeugen, das zur Identifizierung und Festnahme des Täters führte (INTERPOL, 2008).

Die kriminalistische Bedeutung lag auch in dieser Phase nicht in einem einzelnen Verfahren, sondern in der Kombination mehrerer Ansätze. Die polizeitechnische Reaktion auf digitale Bildfälschungen zwischen 2000 und 2010 bestand damit in der Etablierung eines neuen forensischen Blicks auf das digitale Bild. Es war nun nicht mehr nur Abbild, sondern zugleich Datei, Datensatz und Spurenträger. Gerade darin lag gegenüber der klassischen Bildbetrachtung der entscheidende Fortschritt der Polizeitechnik dieser Jahre.

Phase 2 – Plattformen, Smartphones und Alltagsfälschungen

In der zweiten Phase zwischen 2010 und 2017 veränderten sich weniger die einzelnen Bildbearbeitungswerkzeuge als vielmehr die Umweltbedingungen, unter denen digitale Bilder entstanden und verbreitet wurden. Photoshop, GIMP und andere Programme wurden zwar stets weiterentwickelt und zunehmend nutzerfreundlicher, die eigentliche handwerkliche Manipulation von Bildmaterial blieb aber im Kern weiterhin eine Tätigkeit von Kopieren, Retuschieren und Anpassen. Der entscheidende Unterschied zur ersten Phase lag daher nicht in einer völlig neuen Fälschungstechnik, sondern in der massenhaften Verfügbarkeit von Bildmaterial, der mobilen Entstehung digitaler Spuren und der Verbreitung über soziale Netzwerke.

Die Abgrenzung der hier gebildeten Phasen ist selbstverständlich nicht trennscharf. Es gab 2010 keinen technischen Einschnitt, ab dem plötzlich eine neue Form der digitalen Bildfälschung begann. Vielmehr handelt es sich um einen fließenden Übergang: Die Werkzeuge der ersten Phase blieben weiterhin nutzbar, während sich gleichzeitig die Entstehungs- und Verbreitungsbedingungen digitaler Bilder grundlegend veränderten. Das iPhone war in Deutschland bereits seit 2007 erhältlich, Facebook und YouTube gehörten schon lang zu den Massendiensten des Netzes, die eigentliche kriminalistische Verdichtung trat aber erst mit der massenhaften Verbreitung mobiler Internetnutzung, sozialer Netzwerke und kamerafähiger Smartphones ein (Koch & Frees, 2015).

Diese Veränderung lässt sich an wenigen Zahlen verdeutlichen: Während die mobile Internetnutzung 2010 noch bei 13 Prozent der Nutzenden lag, stieg sie bis 2015 auf 55 Prozent, bei den 14- bis 29-Jährigen sogar auf 81 Prozent (Koch & Frees, 2015). Parallel wurde das Smartphone zum zentralen Alltagsgerät: 2017 nutzten laut Bitkom 78 Prozent der Bevölkerung ab 14 Jahren in Deutschland ein Smartphone; von diesen Nutzenden verwendeten

90 Prozent das Gerät als Kamera und 68 Prozent für soziale Netzwerke (Bitkom, 2017). Das Smartphone wurde dadurch neben dem Telefon gleichzeitig zur Kamera, zum Veröffentlichungsmedium und somit auch zum potenziellen Spurenträger.

Das deutschlandweit genutzte mobile Datenvolumen stieg zwischen 2008 und 2017 dabei um mehr als das Hundertfache (Bitkom, 2017; Bundesnetzagentur 2018). Diese Zunahme verdeutlicht nicht nur den rasanten Ausbau mobiler Kommunikation, sondern auch die explosionsartige Vermehrung potenzieller digitaler Spuren. Jeder Datentransfer, jede mobile Nutzung und jede plattformbasierte Interaktion erzeugte zusätzliche Verkehrs-, Nutzungs- oder Inhaltsdaten, die für kriminalistische und forensische Analysen relevant werden konnten.

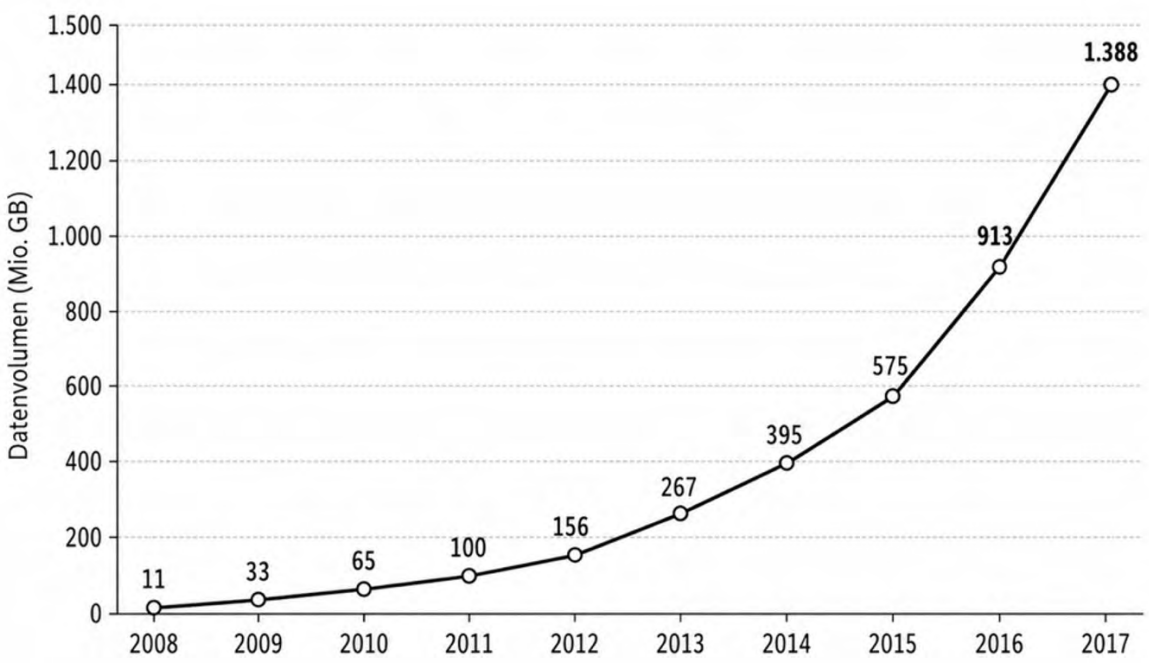


Abb. 4: Mobiles Datenvolumen im deutschen Mobilfunk, 2008–2017. Eigene Darstellung, Datengrundlage Bitkom (2017); Bundesnetzagentur (2018).

Von der Bildmanipulation zur Kontextfälschung

Für digitale Fälschung bedeutete dies eine erhebliche Ausweitung des Ausgangsmaterials und somit der absoluten Anzahl digitaler Spuren. Fotos existierten nicht mehr nur auf Digitalkameras, lokalen Festplatten oder einzelnen Computern, sondern in sozialen Netzwerken, Messengern, Cloudspeichern, Verkaufsplattformen und Datingprofilen. Gleichzeitig wurden Bild-, Orts- und Profildaten enger mit personenbezogenen Daten verknüpft (Poller & Waldmann, 2013).

Damit verlagerte sich die Manipulation häufig vom Bildinhalt auf den digitalen Zusammenhang. Täter mussten Bildmaterial nicht mehr zwingend selbst herstellen, sondern konnten vorhandene Bilder kopieren, aus dem Kontext lösen und neu verwenden. Die Fälschung bestand dann nicht mehr allein in einer bearbeiteten Datei, sondern in einer plausiblen, künstlichen, digitalen Identität inklusive Profilbild, Name, Lebenslauf, Freundesliste, E-Mail-

Verlauf oder Zahlungsbelegen. Gerade deshalb wurde in dieser Phase nicht mehr nur die überzeugende Fotomontage kriminalistisch relevant, sondern die Fälschungen wurden in eine digitale Interaktion über Chats, Anzeigen, Profile und soziale Beziehungen glaubwürdig eingebettet und wirkten so als Gesamtbild. Das BKA stellte diesen Diebstahl digitaler Identitäten 2013 als aktuelles Phänomen im Bundeslagebild Cybercrime besonders heraus (BKA, 2013). Der Wissenschaftliche Dienst des Bundestages nannte 2014 als typische Einsatzbereiche solcher gestohlenen Identitäten unter anderem Bestellungen im Online-Handel, Kreditkartenmissbrauch und den Zugriff auf fremde Online-Banking-Konten (Trips-Hebert, 2014). Auch das Love-Scamming ist seit mindestens Mitte der 2010er Jahre als Deliktsmuster etabliert und gilt als Beispiel für die Professionalisierung von Online-Betrug und der Verlagerung von organisierter Kriminalität ins Internet (Verbraucherzentrale, 2017; BKA, 2018).

Dass Online-Identitätsmissbrauch nicht nur zu finanziellen Schäden führen kann, zeigen mehrere Fälle der deutschen Kriminalgeschichte: Beim sog. Güstrower „Facebook-Mord“ an Sophie W. (2018) gewann der Täter über ein Fake-Facebook-Profil namens „Mike Müller“ erneut das Vertrauen seiner Ex-Partnerin und nutzte das geplante Blind Date zur Tötung (dpa, 2018). Auch im Berliner Fall um Claus Brunner legte dieser ein Fake-Profil mit dem Namen seines späteren Mordopfers an, damit sie auf ihn aufmerksam wurde (Dassler, 2016).

Skalierung und Professionalisierung digitaler Fälschungspraxis

Ab etwa 2013 professionalisierten sich zudem die kriminellen Infrastrukturen. Große Datenlecks, Malware, Botnetze, Darknet-Marktplätze und digitale Zahlungswege begünstigten eine Arbeitsteilung, bei der Täter nicht mehr alle technischen Fähigkeiten selbst besitzen mussten. Außerdem konnten Fälschungen und gestohlene Identitäten durch den Ausbau der delinquenten Internetstrukturen (vor allem Darknet-Handelsplätze, Bulletproof-Hosting und Geldwäschedienste) online zum Verkauf angeboten werden (BKA, 2013; Europol, 2015).

Gleichzeitig sanken die Einstiegshürden durch bessere Verfügbarkeit von Werkzeugen, Anleitungen und kriminelle Dienstleistungen (BKA, 2014). Für die Fälschungspraxis verschob sich damit die erforderliche Kompetenz: Die saubere Bearbeitung eines Fotos oder eines Ausweisdokuments erforderte weiterhin handwerkliches Geschick; die kriminelle Gesamtleistung lag aber zunehmend in einer Kombination aus echten gestohlenen Daten, nachgebauten Dokumenten, glaubwürdigen Profilen und stimmiger Kommunikation im Plattformkontext.

Erschwerend kam in dieser Periode die simple Wiederholbarkeit des Tatgeschehens hinzu. Während klassische Bildfälschungen häufig auf ein einzelnes Bild und einen bestimmten Verwendungszweck ausgerichtet waren, konnten digitale Fälschungen nun massenhaft reproduziert, leicht verändert und in verschiedenen Kontexten erneut verwendet werden. Biagioli beschreibt diese Entwicklung treffend:

> *„Und obwohl Fälschen nach wie vor Handarbeit ist, können einzelne Betrüger dank digitaler Hilfsmittel eine quasiindustrielle Produktivität erreichen.“* (Biagioli, 2019)

Zugleich entstanden durch Smartphones neue Spuren, die digitale Lichtbilder für Ermittlungen wertvoll machten. Die Bilddatei enthielt nicht nur Pixel, sondern auch Metadaten, bspw. über Aufnahmezeit, Gerät, Software und GPS-Informationen. Solche Informationen waren aber zugleich veränderbar, löschbar oder durch Plattformprozesse nicht mehr vorhanden. Denn während Smartphones die Menge potenziell auswertbarer Spuren erhöhten, machten soziale Plattformen diese Spuren zugleich brüchiger. Bilder, die über soziale Netzwerke hochgeladen wurden, wurden häufig umbenannt, verkleinert, neu komprimiert oder von Metadaten befreit (IPTC, 2013; Moltisanti et al., 2015).

Polizeitechnische Antwort: Strukturen, OSINT und Hashwerte

Die polizeitechnische Reaktion auf diese zweite Phase bestand daher nicht nur in Neuerungen in der Bildforensik, sondern in der Ausweitung des digitalen Ermittlungsblicks. Entscheidend war nicht mehr nur, ob ein einzelnes Bild manipuliert worden war, sondern welche Version des Bildes vorlag: Originaldatei, Screenshot, Messenger-Kopie, Plattformkopie, Re-Upload usw. Eine Plattformkopie konnte klassische Spuren wie Exif-Daten, Kamerainformationen oder Sensorrauschen zerstören, aber dafür Hinweise auf Uploadprozesse, Dateibenennung, Kompressionsgeschichte oder Verbreitungswege enthalten. Das digitale Lichtbild wurde damit von einer einfachen Datei zum Teil einer digitalen Überlieferungskette (IPTC, 2013; Moltisanti et al., 2015).

Dieser Perspektivwechsel schlug sich auch organisatorisch nieder. Die Polizei musste ihre Auswertungskompetenzen stark erhöhen und neben der Auswertung von Computern, Kameras und Speichermedien zunehmend auch internetbezogene Tatstrukturen ausermitteln. Auf europäischer Ebene nahmen 2014 Europol, das BKA und weitere internationale Partner die Arbeit in der Joint Cybercrime Action Taskforce auf. Die Bundesregierung beschrieb dies als Reaktion auf die gestiegenen Herausforderungen bei der Bekämpfung von Computer- und Internetkriminalität (Deutscher Bundestag, 2014). Auch auf Landesebene entstanden spezialisierte Strukturen, bspw. Cybercrime-Competence-Center und Fachkommissariate. Parallel gewann die Auswertung öffentlich zugänglicher Internetinformationen an Bedeutung, sodass die klassische Bildforensik und Internetermittlung um den Schwerpunkt OSINT erweitert wurde. Damit verlagerte sich die Ermittlung weg vom eigentlichen Bild zur Frage danach, wo ein Bild zuerst auftauchte, in welchen Profilen es wiederverwendet wurde, ob Aufnahmeort und Aufnahmezeit plausibel waren, usw. (Rüdiger & Rogus, 2014). Ein weiterer Bestandteil der polizeilichen Reaktion war der Umgang mit Masse. Da Bilder millionenfach produziert und verbreitet wurden, konnte die polizeiliche Auswertung nicht mehr allein auf manueller Einzelbetrachtung beruhen. Hash- und Ähnlichkeitssuchverfahren gewannen deshalb an Bedeutung. Insbesondere das Programm PhotoDNA, das 2009 von Microsoft gemeinsam mit dem College Dartmouth entwickelt wurde, gilt als Meilenstein in der Bearbeitung von Big Data. Es berechnet aus Bildern individuelle Hashwerte, die mit denen anderer Bilder abgeglichen werden können und sogar robust gegen Veränderungen an der Bilddatei sind. Es wurde zunächst entwickelt, um bekannte Darstellungen von sexueller Gewalt gegen Kinder wiederzuerkennen, später aber in allen bildbasierten Kriminalitätsbereichen eingesetzt (Ith, 2015).

Zusammenfassend liegt die kriminalistische Bedeutung dieser Phase insbesondere in der Plattformisierung digitaler Bilder. Digitale Fälschungen wurden weiterhin vor allem retuschiert, manipuliert und im Kontext verschoben. Neu war aber, dass die Fälschungen in

einem massenhaft vernetzten, mobilen und plattformabhängigen Kommunikationsraum zirkulierten. Die Polizei reagierte auf diese Veränderungen mit strukturellen Anpassungen und besonders dadurch, dass sie Lichtbilder nicht mehr nur als manipulierte Dateien untersuchte, sondern als flüchtige, kopierbare und kontextabhängige Spuren.

Phase 3 – KI und Deepfakes

Als der Reddit-User u/deepfakes 2017 erstmals massenhaft sexualisierte Videos mit ausgetauschten Gesichtern veröffentlichte, markierte dies einen Wendepunkt in der Geschichte der digitalen Fälschungen. Während Manipulation in der ersten Phase vor allem als handwerkliche Bearbeitung einzelner Dateien und in der zweiten Phase als plattformbasierte Kontextverschiebung verstanden werden konnte, veränderte sich nun der technische Kern der Fälschung selbst. Technologisch beruht diese neue Phase nicht mehr nur auf Bildbearbeitung, sondern auf der Fähigkeit neuronaler Netze, visuelle und auditive Muster zu erlernen und neu zu erstellen. Der Unterschied zu den vorherigen Phasen liegt damit nicht nur in besserer Qualität: Es ist nun nicht nur möglich, ein Bild zu verändern oder schnell zu verbreiten, sondern Personen als scheinbar selbst handelndes, sprechendes und reagierendes Subjekt synthetisch zu erzeugen. Damit wird nicht nur eine Datei gefälscht, sondern eine beobachtbare Wirklichkeit simuliert (Lippitz, 2024).

Dabei ist schon die Funktionsweise der Erstellungs-KI selbst die größte Herausforderung für die Detektion: Deepfakes beruhen auf sog. Generative Adversarial Networks (GANs), die aus zwei miteinander konkurrierenden neuronalen Netzen bestehen: einem Generator und einem Diskriminator. Der Generator kann Inhalte produzieren, der Diskriminator kann überprüfen, ob ein Material synthetisiert oder authentisch ist. Die beiden Netze werden dann in einem fortlaufenden Wechselspiel optimiert. Gelingt es dem Diskriminator, ein erzeugtes Bild oder Video als künstlich zu identifizieren, verändert der Generator die Ausgabe so lang, bis die Inhalte vom Kontrollsystem nicht mehr als Fälschung eingeordnet werden. Anschließend kann der Diskriminator mit weiteren Echtdaten trainiert werden, um seine Kontrollfähigkeiten zu verbessern. Dieser iterative Trainingsprozess setzt sich fort, bis praktische Grenzen erreicht sind, etwa durch die Menge des verfügbaren Trainingsmaterials oder durch die eingesetzten Rechenkapazitäten (Goodfellow et al., 2014). Daraus folgt, dass Systeme zur Erzeugung von Deepfakes strukturell immer auch eine Komponente der Deepfake-Erkennung enthalten. Gerade dieses interne Gegeneinander von Erzeugung und Prüfung führt dazu, dass externe forensische Detektionssysteme vor erhebliche Schwierigkeiten gestellt werden, um synthetische Medien dauerhaft zuverlässig zu identifizieren.

Inzwischen werden neben GANs auch andere Verfahren genutzt, um unterschiedliche Ergebnisse zu erzielen: Face Swap ersetzt das Gesicht einer Zielperson in bereits vorhandenem Bild- oder Videomaterial durch das Gesicht einer anderen Person. Facial Reenactment, Lip Sync oder Motion Transfer übernehmen Mimik, Mundbewegungen oder Bewegungsabläufe, sodass eine reale Person scheinbar andere Worte spricht oder fremde Gesten bzw. Bewegungen ausführt. Voice Cloning reproduziert Stimmen synthetisch, entweder durch Text-to-Speech oder durch Voice Conversion auf der Grundlage von Referenzaufnahmen. Schließlich treten vollgenerierte Inhalte hinzu, bei denen Bild-, Ton- oder Videowirklichkeiten ganz neu erzeugt werden und kein reales Ausgangsereignis mehr existiert (Fraunhofer, 2024).

Die Verbreitung von Deepfakes hat innerhalb weniger Jahre deutlich zugenommen. Ihre technische Entwicklung betrifft dabei nicht nur verschiedene Medienformate, sondern folgt übergreifend gleichen Linien:

- Gesteigerter Realismus bzw. Qualitätssteigerung
- Sinkender Trainingsaufwand, zeitlich und bei Datenanforderungen
- Verkürzte Rechendauer bei der Erzeugung der Inhalte
- Bessere Zugänglichkeit durch benutzerfreundliche Anwendung
- Zunehmende Ausweitung möglicher Einsatzfelder

Diese fünf Veränderungen schreiten mit einer so hohen Entwicklungsgeschwindigkeit voran, dass Deepfakes inzwischen mit minimalen Referenzdaten und sogar Echtzeitübertragungen möglich sind und weder Detektoren noch Menschen die Inhalte sicher als gefälscht erkennen können. Das Fraunhofer Institut beschreibt die Problematik wie folgt:

> *„Mit einem einzigen Foto und einer kurzen Tonspur können Menschen Dinge in den Mund gelegt werden, die sie nie gesagt haben. Wenige Sekunden Original-Sprachaufnahmen genügen, um gefälschte Mitschnitte eines vermeintlich konspirativen Telefonats zu generieren. Vorbei die Zeit, in der man den eigenen Sinnen noch vertrauen konnte.“* (Fraunhofer, 2024)

Deepfakedelinquenz

Deepfakes sind kriminalistisch nicht nur als Medienfälschungen, sondern als digitale Tatmittel innerhalb sozialer und technischer Verbreitungsketten zu betrachten. Ein einzelnes synthetisches Video kann, insbesondere im sexualisierten Kontext, bereits für sich genommen erheblichen Schaden verursachen. Eine verstärkte Wirkung entsteht häufig jedoch erst durch vor- und nachgelagerte Schritte, die mit der Beschaffung von Bild-, Audio- oder Profildaten beginnen, über die synthetische Erzeugung oder Modifikation führen und erst in der Einbettung in einen Kommunikationsprozess (bspw. Videokonferenz, Messenger oder Posts auf Plattformen) ihren eigentlichen Taterfolg entfalten. Die Abbildung 5 verdichtet diese in den Fall- und Lageberichten beschriebene Kette zu einem kriminalistischen Grundschema, in dem das künstlich erzeugte Medium nur ein Glied innerhalb eines umfassenderen sozialen und technischen Täuschungsprozesses ist. Für die polizeiliche Bewertung ist deshalb nicht nur die Herstellung des synthetischen Mediums relevant, sondern ebenso seine Beschaffungsvorgeschichte, seine technische Erzeugung, seine Verbreitungswege und die Rolle sekundärer Weiterverbreiter (Europol, 2022; Rückert et al., 2025).

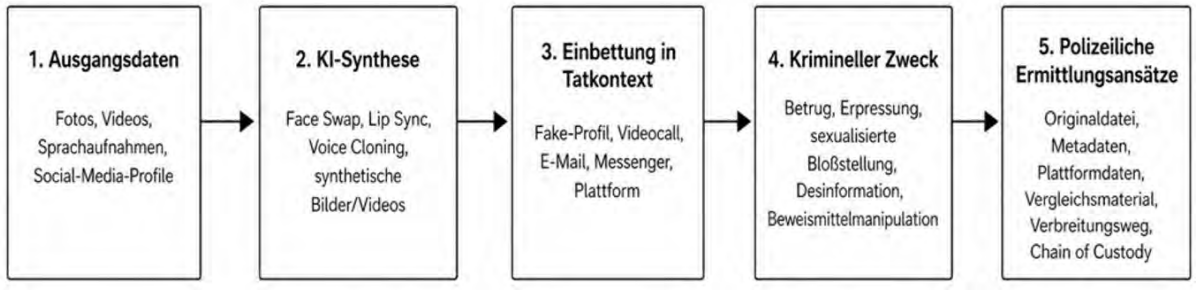


Abb. 5: Deepfakes als kriminalistischer Prozess. Eigene Darstellung.

Ein Fall aus Hongkong verdeutlicht diese Logik für die Betrugsdelikte exemplarisch: Ein Mitarbeiter wurde nach einer Phishing-Nachricht in eine vermeintlich vertrauliche Gruppen-Videokonferenz eingebunden. Dort traten mindestens fünf synthetisch nachgebildete Personen auf, deren Erscheinungsbild offenbar auf öffentlich verfügbaren Videoaufnahmen beruhte. Im Vertrauen auf die Authentizität der Gesprächssituation veranlasste der Mitarbeiter anschließend Überweisungen in Höhe von umgerechnet rund 22 Millionen Euro (Government of Hong Kong, 2024). Branchennahe Reports zeigen, dass dies kein Einzelfall ist: En-trust meldete für 2025 weltweit einen Deepfake-Versuch etwa alle fünf Minuten (Entrust, 2026), gegenüber Signicat gaben 71 % der dort befragten Unternehmen an, dass bei den meisten Identitätsbetrugsfällen gegen sie KI eingesetzt werde (Signicat, 2025), und Pindrop beschrieb für audiospezifischen Betrug einen Anstieg von Deepfake-Fraud um 475 % im Jahr 2024 (Pindrop, 2025).

Ein neuerer Modus Operandi bei der Deepfakedelinquenz sind die sog. KYC-Threats. Dabei werden die digitalen Identitätsprüfungen des Know-Your-Customer-Verfahrens mittels KI-Software überwunden, sodass sich ein Deepfake-Avatar bspw. gegenüber einer Bank als Person authentifizieren kann. Die US-Finanzaufsicht warnt in diesem Zusammenhang vor einer Zunahme von manipulierten Ausweisdokumenten, generierten Fotos und Videos, dem Einsatz von Drittanbieter-Webcam-Plugins, fingierten technischen Störungen bei Live-Verifikationen, verweigerter Mehrfaktor-Authentifizierung sowie Widersprüchen zwischen Identitätsdokument und manipulierten Geräte- und Geodaten (FinCEN, 2024). Der Missbrauch richtet sich dabei nicht nur gegen die Plattform als Ganzes, sondern auch gegen den vertrauensstiftenden Kern des Authentifizierungsmechanismus an sich.

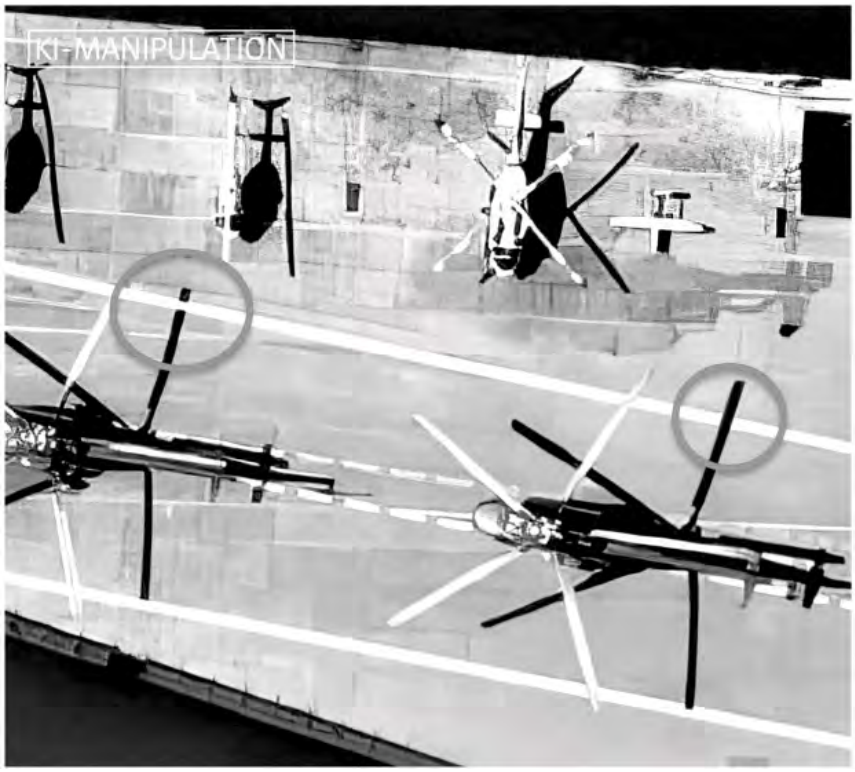


Abb. 6: Bild des iranischen Flugzeugträgers, in der kreisförmigen Markierung: Schatten liegt unter- bzw. oberhalb der Linie. Spiegel, 2026b.

Auch bei der politischen Einflussnahme zielen Deepfakes häufig auf Vertrauenserschütterung, Verunsicherung und die Steuerung öffentlicher Diskurse. Im Januar 2024 kursierten in den USA automatisierte Anrufe, die mit der Stimme von Joe Biden auftraten und die Wählenden von der Teilnahme an der Wahl abhalten sollten (FCC, 2024). Im Spiegel tauchten im März 2026 durch KI manipulierte Bilder auf, die u. a. iranische Flugzeugträger, Explosionen in Teheran und den neuen Obersten Führer des Iran zeigten (Spiegel, 2026b). Nach einem Gutachten wurden die Bilder vom Magazin entfernt. Dass sie zunächst trotz professioneller Redaktion veröffentlicht wurden, zeigt jedoch deutlich: Deepfakes sind nicht nur ein technisches Problem, sondern ein Pro-blem von Prozessen, Verantwortung und Medienkompetenz.

Zwar können nicht einvernehmliche Deepfakepornos (NEDP) auch zur Erpressung, Einschüchterung oder Kontrolle eingesetzt werden, ihr Schadenseintritt entsteht jedoch nicht erst bei einer solchen Anschlussverwendung. Bereits die Erstellung, Androhung oder mögliche Verbreitung kann für Betroffene eine erhebliche Belastung darstellen. Beschrieben werden insbesondere psychische und soziale Folgen wie Angst, Depression, Scham, Stigmatisierung sowie berufliche Nachteile bis hin zum Arbeitsplatzverlust (Ajder et al., 2019; Maddocks, 2020). Der Fall um Collien Fernandes zeigt dies deutlich: Von der Moderatorin und Schauspielerin kursierten KI-generierte pornografische Darstellungen, bei denen ihr reales Gesicht auf fremde Körper montiert wurde. Fernandes bezichtigt ihren Ex-Mann Christian Ulmen der Verbreitung solcher Aufnahmen und gibt an, er habe sie „virtuell vergewaltigt“ (Spiegel, 2026a). Der Fall löste insbesondere in Deutschland eine Diskussion aus, da Fernandes in Ermangelung einer deutschen Rechtsgrundlage in Spanien Anzeige erstattete. Das Problem um solche NEDP wird außerdem dadurch verstärkt, dass sich einschlägige Pornografiewebsites automatisiert spiegeln (sog. Fuskering), was die Entfernung einmal veröffentlichten Materials stark erschwert (Ballon, 2021).

Beweisrechtliche, forensische und kriminalistische Probleme

Die forensische Herausforderung besteht zunächst im dauerhaften Wettlauf von Deepfake-Erkennung und -Erzeugung. Automatisierte Detektoren können im Labor teils hohe Ergebnisse erreichen, doch ihre Belastbarkeit sinkt, sobald neue Generatorfamilien oder unbekannte Trainingsdaten verwendet werden (Nadimpalli & Rattani, 2022). Auch die Technikfolgenabschätzung des Bundestags hält fest, dass Detektoren sowohl False Negatives als auch False Positives anzeigen, sodass sie lediglich Verdachtsmomente, aber keinen gerichtsfesten Beweis liefern können (Deutscher Bundestag, 2026). Außerdem ist die menschliche Komponente als Kontrollinstanz nur eingeschränkt belastbar. So zeigen inzwischen Fälle, dass sogar Sachverständige Deepfakes nicht mehr treffsicher als solche erkennen können (Rahman et al., 2022). In einer Studie des Fraunhofer Instituts schnitten IT-Fachkräfte sogar nicht besser als Laien ab (Fraunhofer, 2025).

Für die Beweisführung im Strafverfahren ist daraus eine doppelte Pro-blemlage entstanden. Erstens wird der hohe Beweiswert von audio-visuellen Beweisen angreifbar, zweitens entsteht die Gefahr, dass auch authentische Aufnahmen mit dem bloßen Verweis darauf, dass es sich um eine Fälschung handeln könnte, anfällig für Diskreditierungen sind (Deutscher Bundestag, 2026).

Kriminalistisch besonders folgenreich ist schließlich, dass die Spurenlage multimodal geworden ist. Ein Deepfake-Ereignis besteht regelmäßig nicht nur aus Bild, Ton oder Video, sondern aus Datei, Plattform, Account, Kontext, Zahlungsfluss und anschließender Weiterverbreitung durch Dritte. Für Ermittlungen bedeutet das: Deepfake-Fälle verlangen nicht nur Medienforensik, sondern integrierte Fallbearbeitung mit Cybercrime, klassischer Kriminaltechnik, OSINT, Finanzermittlung und Opferhilfe. Deshalb ist die Vorstellung eines Deepfake-Detektors als alleinige Lösung verfehlt; erforderlich ist ein Prozess, der Forensik mit technischen und sozialen Schwerpunkten kombiniert (Lippitz, 2024).

Aktuelle polizeiliche Reaktionen

Die polizeiliche Reaktion in Deutschland befindet sich inzwischen sichtbar im Aufbau, ist aber weiterhin stark föderal und punktuell geprägt. Hervorzuheben ist zunächst das LKA Rheinland-Pfalz, das im Februar 2026 einen KI-basierten Deepfake Detektor vorstellte. Die Anwendung soll große Bildbestände automatisiert vorsortieren, wird auf polizeieigener Infrastruktur betrieben und ist für Massendaten ausgelegt. Für die Einordnung wichtig ist dabei nicht nur das Tool selbst, sondern die organisatorische Architektur dahinter: Die Behörde verknüpft fachliche und technische Expertise über die Digitalisierungskooperation DigiKoRP, testet den Einsatz seit März 2026 im Pilotbetrieb und verweist zudem auf ein starkes Ergebnis in einem internationalen behördlichen Ringversuch mit 54 kriminaltechnischen Laboratorien aus 30 Ländern. Dies zeigt, dass polizeiliche Reaktion nicht erst beim konkreten Delikt beginnt, sondern im Aufbau eigener Infrastrukturen sowie von Datenhoheit und Auswertungskompetenz (MI Rheinland-Pfalz, 2026).

Einen zweiten, stärker phänomen- und opferorientierten Ansatz verfolgt das LKA Hessen. Dort wurde zum 1. April 2026 eine zentrale Ansprechstelle für Deepfakes eingerichtet. Hinzu kommen ein landesweites Lagebild, interne Handreichungen für Anzeigenaufnahme und Streifendienst, die Bewertung geeigneter Analyse-Tools, der Ausbau eines landesweiten „Kompetenznetzwerks Deepfake“ sowie eine Verzahnung von Ermittlungsarbeit, Prävention und Opferberatung. Gerade aus kriminalpolitischer Sicht ist dieser Schritt bedeutsam, weil Deepfakes hier nicht nur als technisches Spezialproblem behandelt werden, sondern als Querschnittsphänomen zwischen Cybercrime, digitaler Gewalt und Prävention. Das dürfte für die bundesdeutsche Entwicklung wegweisender sein als jede Einzelsoftware (MI Hessen, 2026).

Im internationalen Vergleich zeigt sich gleichwohl, dass andere Staaten an einzelnen Punkten bereits weiter operationalisiert sind. Die Polizei in Hongkong führt bereits seit 2023 gesonderte Deepfake-Betrug-Statistiken, unterhält ein beratendes Cybercrime-Gremium, entfernt identifizierte Deepfake-Videos proaktiv und koppelt Repression eng mit öffentlichen Warnungen (Government of Hongkong, 2024). In den USA existiert zwar keine einheitliche, wohl aber eine bemerkenswert dichte Verzahnung aus Regulierung, Finanzaufsicht und Standardisierung: FinCEN formuliert Red-Flag-Indikatoren für Finanzinstitutionen, die FCC sanktioniert Wahlmanipulation durch synthetische Stimmen und NIST systematisiert die Leistungsgrenzen technischer Detektoren (FinCEN, 2024; FCC, 2024; NIST, 2024). Europäische Nachbarländer wie Frankreich, Italien und die Niederlande haben bereits seit 2023 dezidierte Gesetze, die behördliches Handeln legitimieren und der Bevölkerung Rechtssicherheit geben (Greif, 2023). Vor diesem Hintergrund ist die deutsche Entwicklung als erkennbar dynamisch, aber noch nicht hinreichend standardisiert zu bewerten.

Handlungsempfehlungen und Prävention

Für Sicherheitsbehörden folgt daraus ein multimodales Programm, das technologische Lösung, strategische Veränderungen und Expertisenaufbau vereint. Technologisch sollte der Schwerpunkt nicht auf Detektoren mit den besten Laborbenchmarktests, sondern auf Generalisierbarkeit und realitätsnahen Datensätzen beruhen. Praktisch folgt aber besonders ein erhöhter Bedarf an Source-First-Strategien: Originaldateien, Quellgeräte, Erstellzeitpunkte, Übertragungsketten usw. werden wichtiger als die Betrachtung später synthetisierter oder plattformbearbeiteter Endprodukte.

Auf strategischer Ebene ist eine stärkere institutionelle Verzahnung erforderlich. Deepfake-Fälle sollten bundesweit nach konsistenten Lagekategorien erfasst werden, damit Betrug, sexualisierte Gewalt, politische Manipulation, KYC-Angriffe und beweisrelevante Fälschungen nicht in verschiedenen Deliktsrubriken unsichtbar bleiben. Außerdem sollten feste Meldewege zwischen Polizei, Staatsanwaltschaften, Plattformen und anderen Unternehmen eingeführt werden, um schnelle Reaktionen und eine empirisch sinnvolle Erfassung zu ermöglichen.

Zunächst gilt es jedoch, den Schwerpunkt auf die Bildungs- und Aufklärungsebene zu legen. Prävention gegen Deepfakes durch einfache Warnhinweise reicht nicht aus. Die Qualität der Fälschungen verlangt neue Routinen und eine adäquate Skepsis gegenüber digitalen Informationen. Der Aufbau von Digitalkompetenz ist unerlässlich, dazu zählen auch im Alltag die Quellenkontrolle, die Betrachtung auf größeren Displays, die Prüfung von Unstimmigkeiten und auch die Einführung von Verifizierung bspw. durch Code-Wörter.

Für die Polizeipraxis ist sowohl ein Grundlagenwissen bei allen Kräften, insbesondere über die Unterscheidung der Deepfake-Arten, notwendig, um Spurenlagen, Schadensrichtung und Detektionsmöglichkeiten schon im ersten Angriff einschätzen zu können. Gleichzeitig ist aber auch der Aufbau spezieller Expertise, bspw. durch Einstellung von Quereinsteigern, erforderlich, um den Herausforderungen fachlich begegnen zu können.

Ausblick

Je weiter sich Deepfakes verbreiten, desto stärker wächst das, was in der Literatur als liar's dividend beschrieben wird: Nicht nur Fälschungen gewinnen an Überzeugungskraft, sondern echte Aufnahmen verlieren an Beweiskraft, weil ihre Authentizität jederzeit pauschal mit dem Verweis auf Deepfake-Software bestritten werden kann. Dieses Phänomen ist für Strafverfolgung, Journalismus und demokratische Öffentlichkeit gleichermaßen gravierend und wird von Chesney und Citron (2019) auf den Punkt gebracht:

> *„Schädigende Lügen sind nichts Neues. Aber die Fähigkeit, die Realität zu verzerren, hat mit Deepfake-Technologie einen exponentiellen Sprung nach vorne gemacht."*

Rechtlich zeichnet sich inzwischen ein belastbarer Rahmen ab, der jedoch noch nicht vollständig geschlossen ist. Auf EU-Ebene verlangt die KI-Verordnung Transparenzpflichten für Anbieter und Verwender bestimmter KI-Systeme; bei Deepfakes ist offenzulegen, dass

Bild-, Audio- oder Videoinhalte künstlich erzeugt oder manipuliert wurden. Die Bundesnetzagentur hebt diese Pflichten bereits in ihrer Übersicht zu Artikel 50 hervor. Hinzu kommt die Richtlinie (EU) 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, die nach der Bundestagsanalyse ausdrücklich auch den Bereich nicht einvernehmlicher pornografischer Deepfakes erfasst und bis 2027 in nationales Recht umzusetzen ist. Auf Bundesebene wiederum hat das Bundesministerium der Justiz 2026 einen Gesetzentwurf zum Schutz vor digitaler Gewalt vorgelegt, der Strafbarkeitslücken gerade bei pornografischen Deepfakes und täuschenden Inhalten schließen soll (Bundesnetzagentur, 2026; Deutscher Bundestag, 2026; BMJ, 2026).

Insbesondere bei den Kennzeichnungspflichten könnte die Durchsetzung jedoch schon daran scheitern, dass auch die Plattformen Deepfakes nicht treffsicher detektieren können.

Für die kommenden Jahre ist zudem mit einer weiteren, insbesondere agentischen Automatisierung zu rechnen. Agentische KI-Systeme verfolgen selbstständig Ziele, treffen Entscheidungen und handeln, ohne dass ein Mensch jeden Schritt steuern muss (OECD, 2026). Es lässt sich also mit hoher Plausibilität ableiten, dass zukünftig nicht nur einzelne Deepfakes, sondern automatisch gesteuerte Kampagnen an Bedeutung gewinnen werden. Agenten werden automatisiert Opfer suchen, Ausgangsmaterial beschaffen, Deepfakes generieren, massenhaft verbreiten und/oder personalisiert kommunizieren sowie in Echtzeit adaptiv nachjustieren. Sowohl für den Einzelnen als auch für Kritische Infrastrukturen und Sicherheitsbehörden bedeutet das insbesondere in Anschlags- oder Krisenszenarien ein ernst zu nehmendes Risiko, weil synthetische Stimmen, Videos und Avatare zur Ablenkung, Überlastung oder Fehlzuschreibung eingesetzt werden können. Diese Stufe ist zwar noch Prognose, aber sie ist inzwischen keine Science-Fiction mehr, sondern die naheliegendste Fortsetzung bereits beobachteter Automatisierungs- und Skalierungstendenzen.

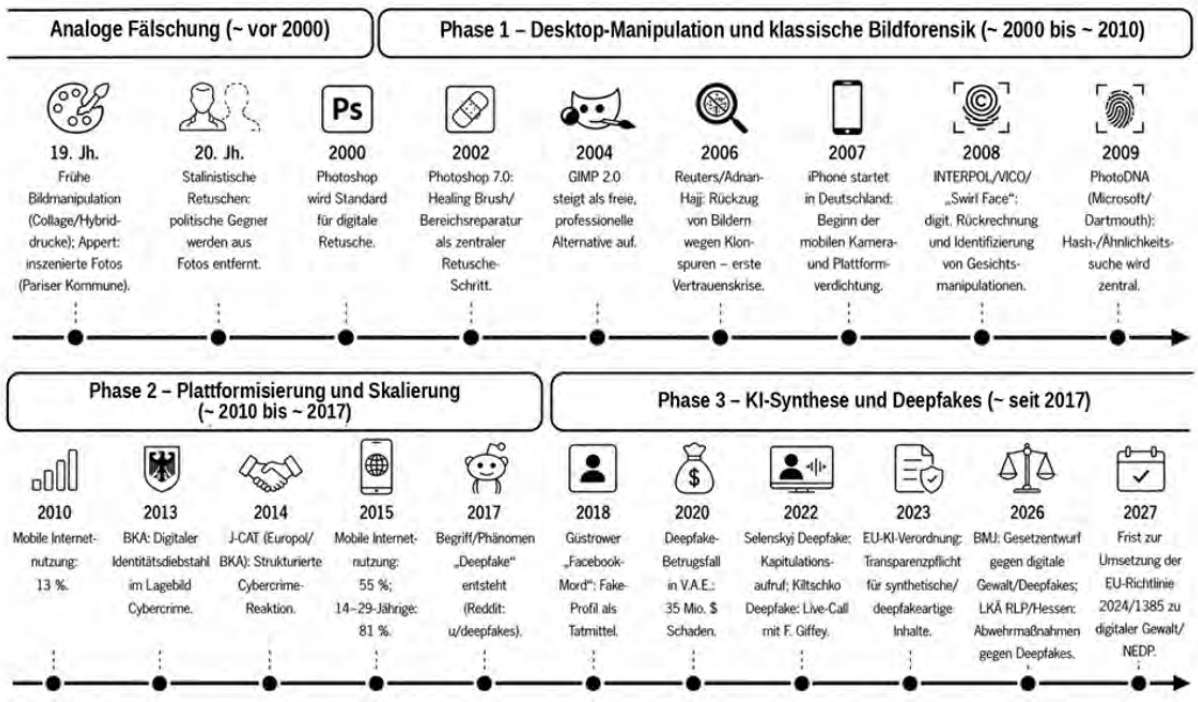


Abb. 7: Zeitleiste der digitalen Fälschungen. Eigene Darstellung.

Fazit

Die Geschichte digitaler Fälschung ist keine Geschichte eines neuen Phänomens, sondern einer technischen Eskalation. Fälschung, Täuschung und Inszenierung begleiteten Bildmedien seit ihren Anfängen. Neu ist jedoch, mit welcher Geschwindigkeit, Skalierbarkeit und Überzeugungskraft solche Fälschungen seit der Digitalisierung hergestellt, verbreitet und in soziale oder wirtschaftliche Prozesse eingebettet werden können. Wer Deepfakes nur als bessere Fälschungen versteht, unterschätzt ihren eigentlichen Kern. Sie sind nicht nur Medien, sondern als Tatmittel geeignet, einen Angriff auf die Infrastruktur moderner Gesellschaften darzustellen.

In ihrer vergleichenden Bewertung verschiedener KI-Technologien gelangen Caldwell et al. (2020) zu dem Schluss, dass Deepfake-Software unter den KI-Anwendungsmöglichkeiten das größte Missbrauchs- und Gefährdungspotenzial aufweist. Deepfakes markieren den Übergang von der digitalen Manipulation einer Einzeldatei zur synthetischen Herstellung von Realität. Sie verändern die Fälschungsproduktion vom handwerklichen Spezialistentum zur für Laien zugänglichen automatisierten App.

Für Kriminalistik, Polizei und Forensik bedeutet das eine Verschiebung vom Datei- zum Prozessverständnis, vom sicheren Urteil zur Wahrscheinlichkeitsbewertung und von der Einzelfallprüfung zur strategischen Vertrauenssicherung. Wenn die Geschichte der digitalen Manipulation die Polizeitechnik eins gelehrt hat, dann dass ein ständiger Perspektivwechsel notwendig ist. Ob dieser nun darin liegen muss, digitalen Beweisen in Zukunft kein Vertrauen mehr zu schenken, wird die Zukunft zeigen. Bis dahin steht die Polizeitechnik vor einer doppelten Aufgabe: Sie muss einerseits Fälschungen technisch besser erkennen, Herkunft und Überlieferung belastbar beweisen und Angriffsszenarien frühzeitig antizipieren. Andererseits muss sie Verfahren schaffen, die auch dann belastbar bleiben, wenn digitale Evidenz nicht mehr selbstverständlich als Abbild der Wirklichkeit akzeptiert wird.

Um dies zu erreichen, genügen technische Lösungen allein nicht aus; erforderlich sind eine engere Zusammenarbeit zwischen Institutionen, klare rechtliche Regelungen, konsequente Aufklärung und Fortbildung – und vor allem eine polizeiliche und gesellschaftliche Haltung, die bei aller Technik den Menschen nicht aus dem Blick verliert.

Referenzen

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The state of deepfakes: Landscape, threats, and impact. Deeptrace.

Biagioli, M. (2019). Vor und nach Photoshop: Rekursiver Betrug im Zeitalter digitaler Reproduzierbarkeit. Angewandte Chemie, 131(46), 17095–17097.

Böhme, R., Freiling, F. C., Gloe, T., & Kirchner, M. (2009). Multimedia-Forensik als Teildisziplin der digitalen Forensik. In S. Fischer, E. Maehle & R. Reischuk (Hrsg.), Informatik 2009 (Lecture Notes in Informatics, Bd. 154, S. 1537–1551). Gesellschaft für Informatik.

Bredenfeld, T. (2008). Adobe Photoshop CS4 – Fortgeschrittene Techniken: 4.2 Fortgeschrittene Einsatzzwecke der Retuschewerkzeuge. Rheinwerk Verlag. https://openbook.rheinwerk-verlag.de/photoshop_cs4/photoshop_cs4_04_retusche_002.htm

Bronx Documentary Center. (o. D.). Adnan Hajj. https://www.bronxdoc.org/bronx-documentary-center/exhibits/altered-images/adnan-hajj/. Abgerufen am 29. April 2026.

Bundeskriminalamt. (BKA) (2013). Bundeslagebild Cybercrime 2013. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013.pdf

Bundeskriminalamt. (2014). Bundeslagebild Cybercrime 2014. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.pdf

Bundeskriminalamt. (BKA) (2018). Romantikbetrug. https://www.bka.de/SharedDocs/Downloads/DE/AktuelleInformationen/Infografiken/ECSM/RomantikBetrug.html

Bundesministerium der Justiz und für Verbraucherschutz (BMJ). (2026, 17. April). Besserer Schutz vor digitaler Gewalt: Bundesjustizministerin stellt Gesetzentwurf vor. https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/0417_Gesetz_gegen_digitale_Gewalt.html

Bundesnetzagentur. (2018). Jahresbericht 2017. https://www.post-und-telekommunikation.de/PuT/1Fundus/Dokumente/Geschaeftsberichte/BNetzA/BNetzA_Jahresbericht_2017-JB2017.pdf

Bundesnetzagentur. (2026). Transparency obligations for AI systems. https://www.bundesnetzagentur.de/EN/Areas/Digitalisation/AI/04_Transparency/start.html

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9(1), Artikel 14. https://doi.org/10.1186/s40163-020-00123-8

Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107, 1753–1820.

Dassler, S. (2016, 23. September). Der Fall Claus-Brunner: Er legte unter dem Namen des Opfers ein Facebook-Profil an. Der Tagesspiegel. https://www.tagesspiegel.de/berlin/er-legte-unter-dem-namen-des-opfers-ein-facebook-profil-an-3758860.html

Deutscher Bundestag. (2014). Bekämpfung von Cybercrime. https://www.bundestag.de/webarchiv/presse/hib/2014_10/333278-333278

Deutscher Bundestag. (2026, 30. Januar). Technikfolgenabschätzung (TA) – Rechtliche und gesellschaftliche Herausforderungen und Potenziale von Deepfakes (Drucksache 21/3952). https://dserver.bundestag.de/btd/21/039/2103952.pdf

Deutsche Presse-Agentur. (2018, 23. August). Rostock – Totschlag in Güs-trow: Prozess gegen 40-jährigen Mann. Süddeutsche Zeitung. https://www.sueddeutsche.de/panorama/rostock-totschlag-in-guestrow-prozess-gegen-40-jaehrigen-mann-dpa.urn-newsml-dpa-com-20090101-180823-99-655444

Dreschler-Fischer, L., & Spitzer, H. (2009). Wie vertrauenswürdig sind Satellitenbilder im Netz? Wissenschaft & Frieden, 27(4), 54–57.

Entrust. (2026). 2026 identity fraud report. https://www.entrust.com/resources/reports/identity-fraud-report

Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

Federal Communications Commission. (FCC) (2024, 30. September). FCC issues $6M fine for N.H. robocalls. https://www.fcc.gov/document/fcc-issues-6m-fine-nh-robocalls

Ferguson, F. (2018, 26. Juni). Finance worker (26) used forged documents to unsuccessfully apply for three loans, court hears. Irish Independent. https://www.independent.ie/irish-news/courts/finance-worker-26-used-forged-documents-to-unsuccessfully-apply-for-three-loans-court-hears/37047659.html

Financial Crimes Enforcement Network. (FinCEN) (2024, 13. November). FinCEN alert on fraud schemes involving deepfake media targeting financial institutions (FIN-2024-Alert004). https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert-508FINAL.pdf

Fraunhofer (2024). Alles Fake!? https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/deepfake.html

Fraunhofer. (2025, 30. September). Wie Künstliche Intelligenz bei der Erkennung von Audio-Deepfakes helfen kann. Institut für Angewandte und Integrierte Sicherheit AISEC. https://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/pressemitteilungen/2025/kuenstliche-intelligenz-erkennt-audiodeepfakes.html

Gilbertson, S. (2008, 15. April). Developer preview shows off the GIMP's new look. WIRED. https://www.wired.com/2008/04/developer-preview-shows-off-the-gimp-s-new-look/

GIMP Development Team. (o. D.). A brief (and ancient) history of GIMP. https://www.gimp.org/about/ancient_history.html

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. Communications of the Association for Computing Machinery, 63(11), 139–144.

Government of the Hong Kong Special Administrative Region. (2024, 26. Juni). LCQ9: Combating frauds involving deepfake. https://www.info.gov.hk/gia/general/202406/26/P2024062600192.htm

Greif, J. (2023). Strafbarkeit von bildbasierten sexualisierten Belästigungen: Eine phänomenologische und strafrechtsdogmatische Betrachtung des sog. Image-based sexual abuse (Dissertation). Ludwig-Maximilians-Universität München.

Herzog, W. (2024). Die Zukunft der Wahrheit. Carl Hanser Verlag.

INTERPOL. (2008). Case study: Interpol working with broadcast media, Operations VICO and IDent. https://www.itu.int/en/cop/case-studies/Documents/Interpol.pdf

International Press Telecommunications Council. (2013, 12. März). IPTC study shows some social media networks remove rights information from photos. https://iptc.org/about-iptc/media-releases/2013-03-12/

Ith, T. (2015, 15. Juli). Microsoft's PhotoDNA: Protecting children and businesses in the cloud. Microsoft News Center. https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/

Kirchner, M. (2006). Digitale Forensik – Spuren in Digitalfotos. Technische Universität Dresden.

Koch, W., & Frees, B. (2015). Unterwegsnutzung des Internets wächst bei geringerer Intensität. Media Perspektiven, 9, 378–382. https://www.ionos.de/digitalguide/fileadmin/DigitalGuide/Downloads/Unterwegsnutzung_des_Internets_waechst_bei_geringerer_Intensitaet.pdf

Lamm, L. (2025, 30. Juni). Fake News in der Antike: Schon die Alten Griechen nutzten Falschinformationen. National Geographic Deutschland. https://nationalgeographic.de/geschichte-und-kultur/2022/09/fake-news-in-der-antike-schon-die-alten-griechen-nutzten-falschinformationen

Lippitz, R. D. U. (2024): Kriminalität und Künstliche Intelligenz: Explorative Analyse der Herausforderungen im Umgang mit Deepfakes in Sicherheitsbehörden. Springer VS. https://doi.org/10.1007/978-3-658-46825-5

Lukáš, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor noise. IEEE Transactions on Information Forensics and Security, 1(2), 205–214.

Macdonald, F. (2024, 13. März). How a 19th-century portrait of Abraham Lincoln was later revealed to be a fake. BBC Culture. https://www.bbc.com/culture/article/20240313-how-a-19th-century-portrait-of-abraham-lincoln-was-later-revealed-to-be-a-fake

Maddocks, S. (2020). "A deepfake porn plot intended to silence me": Explo-ring continuities between pornographic and political deep fakes. Porn Studies, 7(4), 415–423.

Ministerium des Innern und für Sport Rheinland-Pfalz (MI RLP). (2026, 6. Februar). KI-basierter Deepfake Detector stärkt digitale Ermittlungsarbeit der Polizei. https://www.polizei.rlp.de/service/presse/detail/ki-basierter-deepfake-detector-staerkt-digitale-ermittlungsarbeit-der-polizei

Ministerium des Innern, für Sicherheit und Heimatschutz Hessen (MI H). (2026, 26. März). Neue Maßnahmen zur Bekämpfung von sexualisierten Deepfakes. https://www.polizei.hessen.de/meldungen/neue-massnahmen-zur-bekaempfung-von-sexualisierten-deepfakes

Momsen, C., & Hercher, N. (2014). Digitale Beweismittel im Strafprozess: Eignung, Gewinnung, Verwertung, Revisibilität. In Die Akzeptanz des Rechtsstaats in der Justiz (Bd. 37, S. 173–196). Schriftenreihe der Strafverteidigervereinigungen.

Moltisanti, M., Paratore, A., Battiato, S., & Saravo, L. (2015). Image manipulation on Facebook for forensics evidence. In V. Murino & E. Puppo (Hrsg.), Image analysis and processing – ICIAP 2015 (Lecture Notes in Computer Science, Bd. 9280, S. 506–517). Springer. https://vision.unipv.it/CV/materiale2015-16/fifthchoice/92800047.pdf

Nadimpalli, A. V., & Rattani, A. (2022). On improving cross-dataset generalization of deepfake detectors. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 91–99). IEEE. https://doi.org/10.1109/CVPRW56347.2022.00017

National Institute of Standards and Technology (NIST). (2024, November). Reducing risks posed by synthetic content: An overview of technical approaches to digital content transparency (NIST AI 100-4). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf

Organisation for Economic Co-operation and Development. (OECD) (2026, 13. Februar). The agentic AI landscape and its conceptual foundations. https://www.oecd.org/en/publications/the-agentic-ai-landscape-and-its-conceptual-foundations_396cf758-en.html

Paris Musées Collections. (1871). Photomontage mettant en scène l'exécution des « otages de la Commune » avant leur exécution sur le chemin de ronde de la Grande Roquette, le 24 mai 1871. https://www.parismuseescollections.paris.fr/fr/musee-carnavalet/oeuvres/photomontage-mettant-en-scene-l-execution-des-otages-de-la-commune-avant

Pearce, M. (2008, 16. April). Photoshop history. Low End Mac. https://lowendmac.com/software/p/photoshop.html

Pindrop. (2025). Voice intelligence & security report 2025: Synthetic audio fraud and its impact on the financial-services sector. https://www.pindrop.com/research/report/voice-intelligence-security-report

Poller, A., & Waldmann, U. (2013). Soziale Netzwerke bewusst nutzen: Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit. Fraunhofer-Institut für Sichere Informationstechnologie. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Soziale-Netzwerke-2013.pdf

Rabe, F. (2020). Polizeiliche Fotografie: Anforderungen an das Beweismittel „digitales Foto". Die Kriminalpolizei, 4, 14–17.

Rahman, A., Islam, M., Moon, M. J., Tasnim, T., Shahiduzzaman, N. S., & Ahmed, S. (2022). A qualitative survey on deep learning based deep fake video creation and detection method. Australian Journal of Engineering and Innovative Technology, 4(1), 13–26.

Reuters. (2007, 18. Januar). Reuters toughens rules after altered photo affair. https://www.reuters.com/article/economy/reuters-toughens-rules-after-altered-photo-affair-idUSL18678707/

Rückert, C., Hartmann, M., Margerie, M. A., Meinen, L., & Wiedemann, S. (2025). Deepfakes im Straf- und Strafverfahrensrecht. Neue Strafrechtswissenschaft, 315–332.

Rüdiger, T.-G., & Rogus, M. (2014, 1. August). Results of a survey regarding social media utilisation by German police services and police officers: Survey on the use of social media by the German Police. https://hpolbb.de/sites/default/files/field/dokumente/2somep-need_analysis_germany.pdf

Signicat. (2025). The battle in the dark 2025. https://resources.signicat.com/en/the-battle-in-the-dark-report-2025

SPIEGEL. (2026a, 19. März). Collien Fernandes erstattet Anzeige gegen Ex-Mann Christian Ulmen. https://www.spiegel.de/netzwelt/netzpolitik/collien-fernandes-erstattet-anzeige-gegen-ex-mann-christian-ulmen-a-6abfb991-1665-4469-9c8e-3cc5a2cb4f29

SPIEGEL. (2026b, 12. März). Medien: Manipulierte Fotos in Berichten zu Iran entdeckt. https://www.spiegel.de/backstage/medien-manipulierte-fotos-in-berichten-zu-iran-entdeckt-af214eb7a-23dd-4d4b-b6e3-e789f495a9ec

Streck, M., & Draf, S. (2007, 25. März). Entkorkt!: Der große Weinschwindel. stern. https://www.stern.de/wirtschaft/news/entkorkt--der-grosse-weinschwindel-3355208.html

Trips-Hebert, R. (2014, 16. September). Identitätsdiebstahl im Internet: Überblick und rechtliche Implikationen (WD 7-3000-183/14). Deutscher Bundestag, Wissenschaftliche Dienste. https://www.bundestag.de/resource/blob/480340/WD-7-183-14-pdf.pdf

von Lüpke, M. (2014, 13. Oktober). Bildmanipulation: Falsche Fotos vor der Digital-Ära. DER SPIEGEL. https://www.spiegel.de/geschichte/bildmanipulation-falsche-fotos-vor-der-digital-aera-a-996453.html

Verbraucherzentrale. (2017, 24. Oktober). Marktüberblick Online-Dating-Portale. https://www.verbraucherzentrale.de/sites/default/files/2019-11/2017_10_24_marktueberblick_onlinedating_0.pdf

Vormweg, C. (2021, 28. Mai). Vor 150 Jahren: So endete die Pariser Kommune. Deutschlandfunk. https://www.deutschlandfunk.de/vor-150-jahren-so-endete-die-pariser-kommune-100.html

Waschik, K. (2010). Virtual reality: Sowjetische Bild- und Zensurpolitik als Erinnerungskontrolle in den 1930er-Jahren. Zeithistorische Forschungen, 7(1), 30–54. https://doi.org/10.14765/zzf.dok-1795.

Von Computerkriminalität zu Cybercrime – Die Entwicklung im 21. Jahrhundert

Wilfried Honekamp

Die fortschreitende Digitalisierung nahezu aller Lebensbereiche bildet im 21. Jahrhundert die wesentliche Basis des modernen gesellschaftlichen und wirtschaftlichen Lebens (BKA, 2018, 2024). Mit dieser Entwicklung geht jedoch eine fundamentale Transformation krimineller Handlungsmodelle einher: Was zu Beginn des Digitalzeitalters noch als technisches Randphänomen unter dem Begriff der Computerkriminalität wahrgenommen wurde, hat sich zu einer Querschnittsbedrohung entwickelt, die heute unter dem Begriff Cybercrime gefasst wird. Dieser Wandel beschreibt eine tiefgreifende strukturelle Veränderung von der technischen Einzeltat hin zu industriell organisierten, transnational vernetzten Angriffsmodellen (BKA, 2011, 2020a; Atug, 2023). Parallel zu dieser Entwicklung unterliegt auch die polizeiliche Technik einem kontinuierlichen Transformationsprozess. Die Digitalisierung kriminalitätsrelevanter Handlungen erzwingt eine Anpassung der Ermittlungsinstrumente, die datengetrieben, vernetzt und automatisiert ausgestaltet sind. Cybercrime ist ein Treiber für die technologische Weiterentwicklung polizeilicher Arbeit (Povalej et al., 2021; Honekamp et al., 2023).

Der vorliegende Beitrag zeichnet diese Transformation anhand der zentralen polizeilichen Veröffentlichungen nach. Während für die erste Dekade des 21. Jahrhunderts insbesondere die Daten der Polizeilichen Kriminalstatistik (PKS) eine Phase der begrifflichen Konsolidierung dokumentieren, bilden ab dem Jahr 2010 die jährlich erscheinenden Bundeslagebilder Cybercrime des Bundeskriminalamts (BKA) die primäre empirische Grundlage. Diese Berichte verdeutlichen, wie Cyberkriminelle mehr und mehr arbeitsteilig agieren und professionelle Wertschöpfungsketten in der sogenannten Underground Economy etabliert haben (BKA, 2019). Parallel dazu entwickelte sich die forensische Informatik als eigenständiges kriminaltechnisches Feld. Die Sicherung und Auswertung digitaler Spuren, etwa auf Festplatten oder in Netzwerken, wurde zu einer zentralen Voraussetzung erfolgreicher Ermittlungen (Dewald & Freiling, 2015). Diese frühen Entwicklungen bildeten die Grundlage für heutige hochspezialisierte forensische Verfahren, die vermehrt automatisiert und skalierbar ausgestaltet sind (Povalej et al., 2021). Kriminalistisch lässt sich diese Entwicklung als Erweiterung des klassischen Spuren- und Indizienparadigmas verstehen. Die kriminalistische Handlungslehre und Spurenkunde bleiben auch im digitalen Zeitalter anschlussfähig. Digitale Spuren stellen aber aufgrund ihrer Flüchtigkeit, Reproduzierbarkeit, Veränderbarkeit und massenhaften Verfügbarkeit besondere Anforderungen an Sicherung, Interpretation und Kontextualisierung (Plank & Fiedler, 2023). Die Auswertung digitaler Spuren ist daher in kriminalistische Hypothesenbildung, Rekonstruktion von Tatabläufen und beweisbezogene Plausibilitätsprüfung eingebunden. Für die polizeiliche Bearbeitung bedeutete diese Entwicklung, dass digitale Spuren immer häufiger in unterschiedlichen Phasen des Ermittlungsverfahrens berücksichtigt werden mussten. Bereits bei der Anzeigenaufnahme, bei der Sicherung veränderbarer Daten sowie bei der späteren Auswertung entstanden neue Anforderungen an Dokumentation, Beweissicherung und technische Fachkompetenz (Honekamp et al., 2020).

Ein besonderes Augenmerk gilt methodischen Herausforderungen und statistischen Zäsuren. Es muss konstatiert werden, dass polizeiliche Statistiken lediglich das Hellfeld abbilden, während im Bereich Cybercrime von einem weit überdurchschnittlich ausgeprägten Dunkelfeld ausgegangen werden muss (BKA, 2022). Zudem erschweren Veränderungen in den Erfassungsmodalitäten, wie die bundeseinheitliche Umstellung auf das Tatortprinzip im Jahr 2014 oder die Einführung neuer Summenschlüssel, die langfristige Vergleichbarkeit quantitativer Daten. Eine wesentliche Zäsur zur Verbesserung der Analysefähigkeit markierte dabei das Jahr 2008 mit der bundeseinheitlichen Umstellung auf die PKS-Einzeldatensatzanlieferung sowie der Einführung eines detaillierteren sechsstelligen Straftatenschlüssels. Erst durch diese Umstellung wurde auf Bundesebene zudem eine Tatverdächtigenzählung über Bundesländergrenzen hinweg möglich (BKA, 2009). Weitere gravierende Einschnitte bildeten die Umstellung auf das Tatortprinzip im Jahr 2014 sowie die Einführung des Summenschlüssels Cybercrime im Jahr 2021 (BKA, 2015; BKA, 2022).

Neben technologischen Multiplikatoren wie dem Internet der Dinge (IoT) oder Künstlicher Intelligenz (KI) wirkten auch gesellschaftliche Krisen als Katalysatoren der Kriminalitätsentwicklung. Insbesondere die COVID-19-Pandemie schuf durch sprunghafte Digitalisierungsschübe neue Tatgelegenheitsstrukturen, die von Tätern opportunistisch ausgenutzt wurden (BKA, 2020b). Ziel dieses Beitrags ist es, die Entwicklung von der technischen Manipulation einzelner Systeme hin zu einer Perspektive auf digitale Ökosysteme empirisch nachzuzeichnen und in eine langfristige sicherheitspolitische Perspektive einzuordnen. Hierzu wird zunächst die Phase der frühen 2000er Jahre analysiert, bevor der strukturelle Wandel der 2010er Jahre und die aktuellen Herausforderungen durch global agierende Täterkollektive beleuchtet werden.

Die Phase der begrifflichen und strukturellen Konsolidierung (2001–2009)

Die erste Dekade des 21. Jahrhunderts markiert für die deutschen Strafverfolgungsbehörden eine wesentliche Phase der begrifflichen und methodischen Konsolidierung im Umgang mit Straftaten im digitalen Raum. In diesem Zeitraum wurde das Phänomen primär unter dem Sammelbegriff der Computerkriminalität gefasst, wobei die polizeiliche Erfassung im sogenannten Summenschlüssel 8970 erfolgte. Dieser Schlüssel bündelte technische Delikte wie den Computerbetrug (§ 263a StGB), die Datenveränderung und Computersabotage (§§ 303a, 303b StGB) sowie das Ausspähen von Daten (§ 202a StGB). Diese Konsolidierung setzte jedoch nicht voraussetzungslos ein, sondern knüpfte an eine bereits in den 1980er und 1990er Jahren erkennbare statistische und phänomenologische Entwicklung an. Kempa (2006) zeigt für die PKS-Entwicklung von 1987 bis 2003 einen deutlichen Anstieg der erfassten Computerkriminalität von unter 5.000 Fällen im Jahr 1987 auf etwa 80.000 Fälle im Jahr 2003. Zugleich verweist er auf mehrere methodische Brüche, etwa durch die Einbeziehung der neuen Bundesländer ab 1993, durch Veränderungen bei der Erfassung kartengestützter Betrugsformen sowie durch die spätere Aufnahme des Betrugs mit Zugangsberechtigungen zu Kommunikationsdiensten. Bereits diese frühe Entwicklung legt nahe, dass Computerkriminalität statistisch nur begrenzt als kontinuierliche Zeitreihe abbildbar war und dass Veränderungen der Erfassungslogik die polizeiliche Wahrnehmung des Phänomens wesentlich mitprägten.

Statistische Entwicklung und methodische Zäsuren

Die quantitative Entwicklung der Computerkriminalität zwischen 2001 und 2009 war von erheblichen Schwankungen und statistischen Sondereffekten geprägt. Im Jahr 2001 wurden im Bundesgebiet insgesamt 79.283 Fälle registriert, was einem sprunghaften Anstieg von knapp 40 % gegenüber dem Vorjahr entsprach. Diese Dynamik wurde jedoch im Jahr 2002 durch eine grundlegende Änderung der Erfassungsmodalitäten unterbrochen: Durch eine engere Definition beim Betrug mit Debitkarten sank die Zahl der statistisch erfassten Fälle von Computerkriminalität auf dem Papier um 27,5 % auf 57.488 Fälle. In den darauffolgenden Jahren pendelten sich die Fallzahlen zunächst auf einem Niveau zwischen 60.000 und 67.000 Fällen ein (BKA, 2004, 2005, 2008). Zum Ende der Dekade, im Jahr 2009, dokumentierte die PKS jedoch einen gravierenden Anstieg um 17,7 % auf 74.911 Fälle. Dieser Zuwachs resultierte vor allem aus einer deutlichen Zunahme beim Computerbetrug (+35,0 %) sowie beim Ausspähen und Abfangen von Daten (+48,7 %).

Phänomenologische Schwerpunkte der frühen 2000er Jahre

Die Kriminalitätslage dieser Phase war durch spezifische Modi Operandi gekennzeichnet, die die damalige technologische Infrastruktur widerspiegelten:

- Betrug mit Zugangsberechtigungen: Ein signifikanter Anteil der Delikte entfiel auf den Missbrauch von Kommunikationsdiensten, etwa durch Überwindung von SIM-Lock-Sperren oder die Umleitung von Internetzugängen auf kostenintensive 0190er-Verbindungen (BKA, 2002).
- Identitätsdiebstahl und Skimming: Das Ausspähen von Daten entwickelte sich bereits früh zu einem Problemfeld, wobei insbesondere das „Ausspähen der PIN“ an Geldautomaten (Skimming) die Fallzahlen nach oben trieb (BKA, 2004, 2006).
- Softwarepiraterie: In der ersten Hälfte des Jahrzehnts bildete der illegale Handel mit Software und Computerspielen (Softwarepiraterie) einen festen Bestandteil der Computerkriminalität, bevor dieses Feld ab 2006 statistisch an Bedeutung verlor (BKA, 2003, 2006).
- Internet als Tatmittel: Ab 2004 führte das BKA die Sonderkennung „Tatmittel Internet“ ein, um der wachsenden Bedeutung des Netzes über die rein technischen Delikte hinaus Rechnung zu tragen (BKA, 2005). Dabei markierte bereits die Mitte der ersten Dekade den Aufstieg des Betrugs im E-Commerce, insbesondere bei Internetauktionen, womit die Täter ihre Strategien an die gestiegene kommerzielle Nutzung des Netzes anpassten (BKA, 2004, 2005). Bereits 2004 zeigte sich, dass über 50 % aller strafbaren Fälle von Verbreitung pornografischer Schriften mittels Internet begangen wurden (BKA, 2005).
- Erfolg technischer Schutzmaßnahmen: Dass diese eine direkte Auswirkung auf das Hellfeld haben konnten, zeigte sich zudem im Berichtsjahr 2005 beim signifikanten Rückgang des Debitkartenbetrugs im Lastschriftverfahren, welcher primär auf den Erfolg des neu eingeführten Sperrsystems KUNO (Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen) zurückgeführt wurde (BKA, 2006).

Beginnende Professionalisierung

Parallel zur statistischen Erfassung dokumentierten die Sicherheitsbehörden bereits in dieser Phase eine gesteigerte Professionalisierung der Täterstrukturen. Die polizeilichen Lage- und Statistikberichte verweisen für die frühen 2000er Jahre zwar noch überwiegend auf einzelne Deliktsformen wie Computerbetrug, Softwarepiraterie, Ausspähen von Daten oder den Missbrauch von Zugangsberechtigungen, lassen zugleich aber erkennen, dass sich Tatbegehung und Tatgelegenheiten in zunehmendem Maß an globalen Netzinfrastrukturen, internetbasierten Kommunikationsformen und grenzüberschreitenden Verwertungszusammenhängen ausrichteten (BKA, 2002, 2005; Kempa, 2006). Internationale Abkommen wie die Cybercrime-Konvention des Europarats aus dem Jahr 2001 verdeutlichen, dass Cyberdelikte bereits zu Beginn des Jahrhunderts als transnationale Herausforderung verstanden wurden, die eine Harmonisierung rechtlicher Grundlagen und eine engere internationale Zusammenarbeit erforderte (Honekamp et al., 2023).

Parallel dazu wurde das Internet auch aus polizeilicher Sicht immer öfter als eigenständiger Handlungsraum von Strafverfolgung und Gefahrenabwehr wahrgenommen. Siegert (2002) betonte bereits zu Beginn der 2000er Jahre, dass Polizeibeamte, Staatsanwälte und Richter über technisches und soziokulturelles Grundwissen zu den Strukturen des Internets verfügen müssten, um im digitalen Raum angemessen handeln zu können. Seine Differenzierung netzbezogener Straftaten nach netzspezifischen Verbreitungsdelikten, dem Internet als Mittel der Tatkommunikation und dem Internet als virtuellem Tatwerkzeug verweist darauf, dass sich die polizeiliche Perspektive bereits vor der Etablierung der Bundeslagebilder von der klassischen EDV-Kriminalität hin zu internetbasierten Tatmodalitäten erweiterte. Die Phase vor 2010 lässt sich als eine Ära beschreiben, in der Computerkriminalität noch stark über technische Tatmittel und die Manipulation einzelner Systeme definiert wurde, während sich die heutigen komplexen Ökosysteme erst in Grundzügen abzeichneten.

Der Wendepunkt 2010: Etablierung der Bundeslagebilder Cybercrime

Das Jahr 2010 markiert eine entscheidende Zäsur in der polizeilichen Wahrnehmung und Dokumentation digitaler Straftaten in Deutschland. Mit der erstmaligen Veröffentlichung des Bundeslagebildes Cybercrime reagierte das BKA (2011) auf die gestiegene Qualität und Quantität der Bedrohungen, die über die bis dahin gebräuchlichen Kategorien der Computerkriminalität hinausgingen. Dieser Übergang spiegelte die Notwendigkeit wider, ein dynamisches und transnationales Kriminalitätsphänomen systematischer zu erfassen. Die Etablierung dieser Lagebilder ist zugleich Ausdruck einer gesteigerten datenbasierten Polizeiarbeit. Die Zusammenführung, Analyse und Interpretation großer Datenmengen entwickelte sich zu einer zentralen technischen Fähigkeit, die über klassische fallbezogene Ermittlungen hinausgeht und strategische Lagebilder ermöglicht.

Terminologische Neuausrichtung und Definitionsmerkmale

Im Zuge dieser Neuausrichtung wurde der Begriff Cybercrime als umfassende Kategorie etabliert, die alle Straftaten umschließt, welche unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden (BKA, 2011). In der strategischen

Betrachtung erfolgte dabei eine wegweisende Differenzierung zwischen Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne (BKA, 2011, 2018). Diese Differenzierung steht zugleich exemplarisch für ein grundsätzliches Konturierungsproblem des Cybercrime-Begriffs. Plank (2020) zeigt, dass Cyberkriminalität in Forschung und Praxis keineswegs einheitlich bestimmt wird, sondern je nach institutionellem, rechtlichem oder kriminologischem Zugriff unterschiedliche Deliktsbereiche, Tatmittel und Kontrollperspektiven umfasst. Die begriffliche Unschärfe ist dabei nicht nur ein terminologisches Problem, sondern wirkt sich unmittelbar auf Erfassung, Lagebewertung und kriminalpolitische Steuerung aus. Gerade weil digitale Informations- und Kommunikationstechnik sowohl Ziel, Tatmittel als auch Tatkontext strafbarer Handlungen sein kann, bleibt die Grenzziehung zwischen Computerkriminalität, Internetkriminalität und Cybercrime methodisch anspruchsvoll. Als Cybercrime im engeren Sinne werden jene Delikte definiert, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (BKA, 2019). Ein wesentliches Merkmal dieser Deliktsform ist, dass Elemente der elektronischen Datenverarbeitung für die Tatausführung essenziell sind (BKA, 2011). Demgegenüber umfasst Cybercrime im weiteren Sinne Straftaten, bei denen die Informationstechnik primär als Tatmittel zur Planung, Vorbereitung oder Ausführung genutzt wird, wie etwa beim betrügerischen Handel auf Internetplattformen (BKA, 2018, 2019).

Diese seit 2011 etablierte Differenzierung wird jedoch auch kritisch hinterfragt. Honekamp et al. (2023) argumentieren, dass die Unterscheidung zwischen Cybercrime im engeren und weiteren Sinne nicht mehr zeitgemäß ist und künftig entfallen sollte. Während die Abgrenzung ursprünglich dazu diente, die Aufmerksamkeit von Politik und Justiz auf neuartige Ermittlungserfordernisse und Spurenlagen zu lenken, ist Informationstechnik heute ein integraler Bestandteil nahezu aller Lebensbereiche geworden. Da in der polizeilichen Praxis kaum noch Delikte ohne jeglichen Technologiebezug existieren, verliert der Begriff seine Funktion als systematisches Ordnungsmerkmal oder Entscheidungskriterium für Zuständigkeiten. Für die praktische Ermittlungsarbeit folgt daraus, dass digitale Ermittlungskompetenz nicht ausschließlich als Spezialwissen für wenige Cybercrime-Verfahren verstanden werden kann. Vielmehr wird sie zu einer querschnittlichen Anforderung, weil digitale Spuren auch bei Delikten auftreten können, die statistisch oder organisatorisch nicht dem engeren Bereich von Cybercrime zugeordnet werden (Honekamp et al., 2020).

Die Kriminalitätslage im Jahr der Etablierung

Die statistischen Daten des ersten Berichtsjahres unterstrichen die Relevanz dieser neuen Betrachtungsweise. Im Jahr 2010 stieg die Zahl der in der PKS erfassten Fälle von Cybercrime auf 59.839, was einer Zunahme von rund 19 % gegenüber dem Vorjahr entsprach (BKA, 2011). Besonders deutlich trat die wirtschaftliche Dimension hervor: Während die Straftatengruppe des Computerbetrugs mit einem Anteil von rund 46 % das Feld dominierte, verzeichneten die Behörden bei den registrierten Schäden einen sprunghaften Anstieg um mehr als 66 % auf insgesamt 61,5 Mio. Euro (BKA, 2011).

Erkenntnisgrenzen der statistischen Erfassung

Bereits bei der Einführung der neuen Lagebildstruktur wiesen die Sicherheitsbehörden auf die methodischen Grenzen einer rein quantitativen Auswertung der PKS-Daten hin. Es wurde konstatiert, dass eine Bewertung des Phänomens allein auf Basis statistischer Zahlen nicht möglich sei, da relevante Phänomene wie Phishing im Onlinebanking oder gezielte DDoS-Attacken auf Server von Unternehmen oft unter den PKS-Schlüsseln der zugrunde liegenden Einzeltathandlungen, etwa der Erpressung, erfasst werden (BKA, 2010; BKA, 2011). Zudem wurde das Problem des Dunkelfeldes, insbesondere bei der Computersabotage und Datenveränderung, als strukturelles Hindernis identifiziert. Die Behörden gingen bereits 2010 davon aus, dass viele Infektionen von IT-Systemen unentdeckt bleiben oder von geschädigten Unternehmen aus Reputationsgründen nicht zur Anzeige gebracht werden (BKA, 2010). Diese Erkenntnis führte dazu, dass das BKA fortan verstärkt externe Quellen und den kriminalpolizeilichen Nachrichtenaustausch nutzte, um das polizeiliche Hellfeld qualitativ anzureichern (BKA, 2010). Die Etablierung der Bundeslagebilder ab 2010 schuf die empirische und begriffliche Basis, um Cybercrime nicht mehr nur als technisches Problem einzelner Systeme, sondern als komplexe, ökonomisierte und industrielle Form der Kriminalität zu begreifen (BKA, 2011; BKA, 2012).

Struktureller Wandel der Täterstrukturen und Tatmodelle

Der Übergang von der Computerkriminalität zu Cybercrime ist maßgeblich durch eine einschneidende Transformation der Täterstrukturen und der zugrunde liegenden Geschäftsmodelle gekennzeichnet. Während in der Frühphase des 21. Jahrhunderts noch überwiegend hochspezialisierte Einzeltäter das Geschehen dominierten, hat sich das Feld zu einer industriell organisierten, transnational vernetzten Kriminalitätsform entwickelt (BKA, 2010; BKA, 2020a).

Die Underground Economy als infrastrukturelle Basis

Den organisatorischen Kern dieser Entwicklung bildet die Underground Economy, die als globale, virtuelle Schattenwirtschaft fungiert. Hierbei handelt es sich um eine kommerziell ausgerichtete Landschaft, die kriminell genutzte Kommunikations- und Verkaufsplattformen im Internet vereint (BKA, 2020a). Während sich die Szene anfänglich überwiegend in englisch- oder russischsprachigen Foren betätigte, konnte bereits im Jahr 2010 eine breite Etablierung entsprechender Plattformen im deutschsprachigen Raum festgestellt werden (BKA, 2011). Diese Foren dienen dem Austausch von kriminellem Know-how, der Anbahnung von Straftaten sowie dem Handel mit gestohlenen Identitäten und Kreditkartendaten (BKA, 2011; BKA, 2014). Ein Maximum an Anonymität und ein subjektiv geringes Entdeckungsrisiko im Darknet machen diesen Bereich für Täter besonders attraktiv (BKA, 2016; BKA, 2017). Für die Strafverfolgungsbehörden ergibt sich hieraus die Notwendigkeit, verdeckte digitale Ermittlungsansätze zu entwickeln. Dazu zählen insbesondere Undercover-Ermittlungen in geschlossenen Foren, der Einsatz von Open Source Intelligence zur Auswertung öffentlich zugänglicher Daten sowie technische Maßnahmen zur Identifizierung von Infrastrukturen im Darknet. Diese Formen digitaler Ermittlungsarbeit erfordern spezialisierte technische Fähigkeiten und rechtliche Anpassungen.

Ökonomisierung durch Cybercrime-as-a-Service

Ein wesentlicher Treiber der Professionalisierung ist das Modell Cybercrime-as-a-Service (CaaS). Es basiert auf arbeitsteiligen Wertschöpfungsketten, bei denen spezialisierte Akteure einzelne technische Tatbeiträge als Dienstleistung anbieten (BKA, 2018, 2020a). Dies führt dazu, dass die technischen Eintrittshürden für Straftäter sinken, da auch Akteure ohne fundierte IT-Spezialkenntnisse hochkomplexe Werkzeuge oder komplette Infrastrukturen mieten oder kaufen können (BKA, 2011, 2015, 2019). Das Angebot in der Underground Economy reicht dabei von der Vermietung von Botnetzen und DDoS-Attacken bis hin zur Bereitstellung schlüsselfertiger Schadsoftware (BKA, 2014, 2017). Die Täter agieren hierbei immer mehr wie reguläre Wirtschaftsunternehmen und bieten ihren kriminellen Kunden teilweise technischen Support, Updates oder Beratungsdienste an (BKA, 2012, 2018).

Zur systematischen Beschreibung dieser arbeitsteiligen Strukturen hat das BKA ein System von neun essenziellen Säulen identifiziert, die den gesamten Verlauf einer kriminellen Tat abdecken. Den Einstieg bilden digitale Plattformen und Kommunikationskanäle, die als zentrale Treffpunkte fungieren, an denen kriminelle Dienstleistungen angeboten und nachgefragt werden (Säule 1). Weitere Säulen umfassen die Bereitstellung einer widerstandsfähigen technischen Infrastruktur, die polizeilichen Abschaltungen möglichst lange widersteht (Säule 2), den Handel mit gestohlenen digitalen Identitäten und Zugangsdaten (Säule 3) sowie die spezialisierte Erstellung von Schadsoftware, deren gezielte Verfremdung zur Umgehung von Schutzprogrammen und die technische Verteilung dieser Programme auf fremde Systeme (Säulen 4 bis 7). Die kriminelle Kette wird durch Beteiligte abgeschlossen, welche die illegale Beute, etwa Geldbeträge oder Waren, in der physischen Welt abholen und weiterleiten (Säule 8), sowie durch Akteure, die digitale Währungen waschen, um deren Herkunft zu verschleiern (Säule 9). Nur noch wenige Cyberkriminelle begehen ihre Taten heute ohne die wesentliche Unterstützung dieser spezialisierten Drittanbieter (BKA, 2020a).

Diese Entwicklung verschiebt den Fokus polizeilicher Maßnahmen zunehmend von einzelnen Tätern hin zu den zugrunde liegenden technischen Infrastrukturen. Maßnahmen wie die Identifizierung und Abschaltung von Command-and-Control-Servern oder die internationale Koordination zur Zerschlagung krimineller Plattformen gewinnen an Bedeutung (BKA, 2016, 2017, 2018, 2019). So veränderten sich auch die Anforderungen an die Vorbereitung kriminalpolizeilicher Maßnahmen. Neben der Sicherung einzelner Endgeräte gewannen die Rekonstruktion technischer Kommunikationsbeziehungen, die Berücksichtigung verteilter Datenquellen und die frühzeitige Einbindung forensischer Fachkompetenz an Bedeutung (Honekamp et al., 2020). Aktuell zeigt sich, dass diese infrastrukturelle Perspektive inzwischen durch einen mehrdimensionalen Bekämpfungsansatz ergänzt wird. Das BKA (2026) beschreibt eine Strategie, die personenbezogene Ermittlungen, die Zerschlagung technischer Infrastrukturen, den Entzug finanzieller Mittel sowie eine disruptive Kommunikation zur Reputationsschädigung in der cyberkriminellen Szene miteinander verbindet.

Operative Maßnahmen wie die Operation Endgame verdeutlichen dabei, dass Strafverfolgungsbehörden nicht nur einzelne Täter identifizieren, sondern zugleich zentrale Malware-Infrastrukturen, Zahlungswege und Unterstützungsdienste adressieren, um die Funktionsfähigkeit krimineller Wertschöpfungsketten nachhaltig zu schwächen (BKA, 2026). Zugleich verdeutlichen Diskussionen um aktive Gegenmaßnahmen gegen angreifende Infrastruktu-

ren, dass polizeiliche Handlungsfähigkeit im Cyberraum an rechtliche Zuständigkeiten, tatsächliche Umsetzbarkeit und internationale Kooperationsmechanismen gebunden bleibt (Kunze, 2023).

Diese rechtliche Begrenzungs- und Konkretisierungsfrage zeigt sich auch in der aktuellen gesetzgeberischen Initiative. Der Entwurf des Gesetzes zur Stärkung der Cybersicherheit sieht vor, die Cyberabwehr des Bundes durch Änderungen im BSIG, BKAG und BPolG auszubauen. Vorgesehen sind insbesondere Befugnisse zur Untersagung des Betriebs informationstechnischer Systeme, zur Einschränkung, Unterbindung oder Umleitung von Datenverkehr sowie zum Auslesen, Löschen oder Verändern gefahrgegenständlicher Daten in informationstechnischen Systemen. Für das BKA soll zudem eine Aufgabe zur Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik geschaffen werden, wenn schwerwiegende, bundesbezogene oder internationale Gefahrenlagen betroffen sind. Der Entwurf dokumentiert damit, dass sich die polizeiliche Reaktion auf Cybercrime nicht mehr allein auf nachträgliche Strafverfolgung richtet, sondern auch auf die operative Unterbrechung technischer Angriffs- und Täterinfrastrukturen zielt (Bundesregierung, 2026).

Auch organisatorisch spiegelt sich diese Entwicklung in der Zunahme zentraler Ermittlungen wider. Bei wellenförmig auftretenden Cybercrime-Sachverhalten übernehmen einzelne Dienststellen oder Dienststellenverbünde die koordinierte Bearbeitung, um Spuren bundesweit zusammenzuführen, Doppelermittlungen zu vermeiden und Ressourcen zu bündeln. Für 2025 weist das BKA 34 Zentrale Ermittlungen aus, darunter 29 gegen Ransomware-Akteure (BKA, 2026).

Ransomware-Ökosysteme und Affiliate-Modelle

Die industrielle Dimension von Cybercrime tritt besonders deutlich im Bereich der Ransomware hervor. Mit dem Modell Ransomware-as-a-Service vermieten Entwicklergruppen ihre Erpressungssoftware an sogenannte Affiliates, welche die eigentlichen Angriffe gegen Unternehmen oder öffentliche Einrichtungen ausführen (BKA, 2016, 2022). Die erzielten Lösegelder werden nach einem festgelegten Schlüssel zwischen Entwicklern und Operatoren aufgeteilt (BKA, 2020a; Atug, 2023). Atug (2023) beschreibt Ransomware als arbeitsteiliges Geschäftsmodell organisierter Kriminalität. Die ökonomische Logik dieses Modells beruht darauf, dass einzelne Tatbeiträge voneinander getrennt und spezialisiert angeboten werden: Initiale Zugänge zu Unternehmensnetzwerken, technische Infrastruktur, Schadsoftware, Verhandlungsführung, Zahlungsabwicklung und Veröffentlichungsdruck können von unterschiedlichen Akteuren erbracht werden. Dadurch entsteht eine kriminelle Wertschöpfungskette, in der nicht jeder Beteiligte den gesamten Angriff beherrschen muss. Für die Entwicklung von Cybercrime ist dies zentral, weil Ransomware exemplarisch zeigt, wie aus technisch anspruchsvollen Einzelangriffen skalierbare, dienstleistungsförmig organisierte Erpressungsmodelle geworden sind.

Seit dem Jahr 2019 hat sich zudem die Double Extortion als Standard-Modus-Operandi etabliert (BKA, 2020a, 2021). Hierbei werden sensible Daten vor der Verschlüsselung der Systeme exfiltriert, um die Opfer zusätzlich mit der Drohung einer Veröffentlichung auf speziellen Leak-Websites unter Druck zu setzen (BKA, 2020a, 2022). Atug (2023) ordnet diese Entwicklung historisch ein und weist darauf hin, dass der Abgriff und Handel mit Data Leaks bereits

vor dem Aufstieg moderner Ransomware-Gruppierungen existierte. Ransomware-Akteure adaptierten dieses Verfahren jedoch als zusätzlichen Erpressungsmechanismus. Eine besondere Rolle kam dabei der Tätergruppierung Maze zu, die im Jahr 2019 die Veröffentlichung zuvor entwendeter Daten als Druckmittel gegenüber betroffenen Institutionen einsetzte. Durch diese Verbindung von Verschlüsselung, Datenabfluss und Veröffentlichungsdrohung wandelte sich Ransomware von einer primär technischen Verfügbarkeitsstörung zu einem mehrdimensionalen Erpressungsmodell. Große Täterkollektive fokussieren sich dabei vermehrt auf das Big Game Hunting, also gezielte Angriffe auf finanzstarke Organisationen oder Kritische Infrastrukturen, um maximale Schadenssummen zu erzielen (BKA, 2020a, 2021).

Die COVID-19-Pandemie als Zäsur und Beschleuniger (2020–2022)

Die weltweite Ausbreitung des Coronavirus im Jahr 2020 markiert eine tiefgreifende Zäsur in der Kriminalitätsentwicklung des 21. Jahrhunderts. Die Pandemie wirkte nicht als Auslöser völlig neuer Kriminalitätsformen, sondern fungierte als Katalysator und Beschleuniger für bereits bestehende Trends im Bereich Cybercrime (BKA, 2020b, 2021). Durch staatlich verordnete Maßnahmen wie Homeoffice, Social Distancing und die Schließung analoger Angebote verlagerte sich das gesellschaftliche und wirtschaftliche Leben in einem historisch beispiellosen Ausmaß in den digitalen Raum (BKA, 2020b, 2021). Diese sprunghafte Zunahme der digitalen Abhängigkeit schuf aus Sicht der Strafverfolgungsbehörden einen Nährboden für Cyberkriminelle (BKA, 2020b).

Krisen-Narrative und opportunistisches Social Engineering

Ein charakteristisches Merkmal dieser Phase war die hohe Anpassungsfähigkeit der Täter an die gesellschaftliche Ausnahmesituation. Cyberkriminelle nutzten die Sorgen, Unsicherheiten und das gesteigerte Informationsbedürfnis der Bevölkerung gezielt als Narrativ für ihre Angriffe. Etablierte Modi Operandi wie Phishing und Malware-Spamming wurden in kürzester Zeit inhaltlich umgestellt. Ein prominentes Beispiel bildeten gefälschte Webseiten zur Beantragung von Corona-Soforthilfen, auf denen Täter versuchten, sensible Unternehmensdaten für großflächigen Subventionsbetrug auszuspähen. Allein in Nordrhein-Westfalen wurden in diesem Zusammenhang über 1.200 Online-Anzeigen registriert, was zeitweise zum Stopp der staatlichen Auszahlungen führte. Parallel dazu wurden Malspam-Kampagnen identifiziert, die unter missbräuchlicher Nutzung der Identität von Behörden wie der Weltgesundheitsorganisation (WHO) oder dem Bundesministerium für Gesundheit Schadsoftware wie Emotet oder Trickbot distribuierten (BKA, 2020b).

Der digitale Stresstest: DDoS und Angriffe auf die digitale Infrastruktur

Die flächendeckende Verlagerung von Arbeits- und Bildungsprozessen in das Internet führte zu einem Anstieg des Datenverkehrs, was die IT-Infrastruktur einem permanenten Stresstest aussetzte. VPN-Server und Fernzugriffslösungen wurden zu kritischen Elementen für die Aufrechterhaltung der betrieblichen Abläufe und damit zu attraktiven Zielen für Erpressungsversuche. So verzeichneten die Behörden eine deutliche Zunahme und Intensivierung von DDoS-Angriffen, die gezielt darauf abzielten, VPN-Server oder digitale Lernplattformen lahmzulegen (BKA, 2021). Ein signifikanter Vorfall ereignete sich im Schulwesen, als DDoS-

Attacken auf Videokonferenzsysteme und Lernmanagementsysteme wie Moodle den Fernunterricht für Hunderttausende Schüler beeinträchtigten (BKA, 2022). Für die Sicherheitsbehörden ergibt sich daraus die Notwendigkeit, technische Kompetenzen im Bereich der Angriffserkennung, der Analyse von Netzwerkverkehr und der Abwehr koordinierter Angriffe auszubauen. Die Pandemie wirkte insofern auch als Stresstest für die technische Leistungsfähigkeit der digitalen Infrastruktur sowie der entsprechenden Sicherheitsarchitekturen.

Ransomware im Gesundheitswesen: Angriffe auf systemrelevante Ziele

Eine neue qualitative Dimension erreichte die Bedrohungslage durch Ransomware-Angriffe auf das Gesundheitswesen. Täterkollektive erkannten die besondere Verwundbarkeit von Krankenhäusern und Forschungseinrichtungen während der Pandemie und nutzten die Notlage aus, um hohe Lösegelderpressungen durchzuführen. Die Notwendigkeit, die Patientenversorgung unter allen Umständen aufrechtzuerhalten, erhöhte den Druck auf die betroffenen Einrichtungen (BKA, 2020a, 2021). Ein herausragender Fall war der Ransomware-Angriff auf das Universitätsklinikum Düsseldorf im September 2020. Die Verschlüsselung der IT-Systeme führte dazu, dass die zentrale Notversorgung eingestellt werden musste und Patienten auf umliegende Krankenhäuser verteilt wurden, was die potenzielle Gefahr für Leib und Leben durch Cyberangriffe nachdrücklich verdeutlichte (BKA, 2021).

Langfristige Auswirkungen und statistische Entwicklung

Obwohl die spezifischen Fallzahlen mit direktem Corona-Bezug nach Aufhebung der Schutzmaßnahmen im Jahr 2022 zurückgingen, verblieb die Kriminalitätsbelastung im Cyberraum insgesamt auf einem hohen Niveau (BKA, 2023). Die Pandemie hat zu einer dauerhaften Transformation der Arbeitswelt und zu einer weiteren Verfestigung digitaler Arbeits- und Kommunikationsformen beigetragen, wodurch die Angriffsfläche für Cybercrime nachhaltig vergrößert wurde. Die Erfahrungen dieser Jahre unterstrichen die Notwendigkeit einer gesteigerten Cyber-Security-Awareness in allen gesellschaftlichen Bereichen und einer engen Kooperation zwischen staatlichen Sicherheitsbehörden und dem Privatsektor (BKA, 2021).

Technologische Multiplikatoren und neue Angriffsvektoren

Die technologische Entwicklung des 21. Jahrhunderts hat nicht nur die legale digitale Wirtschaft geprägt, sondern wirkt auch im Bereich der Kriminalität als Verstärker bestehender Risiken (BKA, 2024). Während die frühen Jahre der Computerkriminalität noch durch die Manipulation isolierter Systeme geprägt waren, ermöglichen moderne Schlüsseltechnologien den Tätern heute eine deutlich weitergehende Skalierung und Professionalisierung ihrer Angriffe (BKA, 2014, 2018). Diese Entwicklungen betreffen in gleicher Weise die technische Ausstattung der Strafverfolgungsbehörden. Die steigende Komplexität digitaler Infrastrukturen erfordert den Einsatz hochspezialisierter Analysewerkzeuge, etwa zur automatisierten Auswertung großer Datenmengen, zur Erkennung von Angriffsmustern oder zur forensischen Analyse verteilter Systeme. Moderne Polizeitechnik bewegt sich dabei im Spannungsfeld zwischen Datenverfügbarkeit, Analysefähigkeit und rechtlichen Rahmenbedingungen (Povalej et al., 2021; Honekamp et al., 2023).

Das Internet der Dinge und die industrielle Vernetzung

Der Trend zum IoT beschreibt die Vernetzung intelligenter Endgeräte, die über herkömmliche Computer hinausgehen und dauerhaft online sind (BKA, 2014, 2017). Diese Geräte verfügen oft nur über unzureichende Schutzmechanismen oder nutzen veraltete Software, was sie zu einem attraktiven Ziel für Cyberkriminelle macht (BKA, 2014, 2016). Besonders kritisch bewerten die Sicherheitsbehörden die Einbindung dieser Geräte in Botnetze, wie etwa das Mirai-Botnetz, das durch die Nutzung von IoT-Infrastrukturen DDoS-Angriffe mit rasant steigenden Bandbreiten ermöglichte (BKA, 2017). Auch im Kontext von Industrie 4.0 führt die webbasierte Steuerung von Produktionsprozessen zu einer steigenden Abhängigkeit der Wirtschaft von einer funktionierenden IT (BKA, 2015, 2018). Angriffe in diesem Sektor bergen das Risiko kompletter Produktionsstillstände und kaskadenartiger Ausfälle ganzer Lieferketten (BKA, 2016, 2021).

Mobile Endgeräte und soziale Netzwerke

Mobile Endgeräte wie Smartphones und Tablets haben konventionelle Computer in privaten Haushalten weitgehend verdrängt (BKA, 2016, 2018). Da diese Geräte in der Regel ständig online sind und für sensible Transaktionen wie Onlinebanking oder mobile Zahlungsverfahren genutzt werden, sind sie zu einem primären Angriffsziel avanciert (BKA, 2010, 2015). Täter nutzen hierbei speziell auf mobile Betriebssysteme, insbesondere Android, zugeschnittene Malware (BKA, 2015, 2019). Parallel dazu bieten soziale Netzwerke ideale Bedingungen für Social Engineering (BKA, 2012, 2018). Täter nutzen das bestehende Vertrauensverhältnis zwischen Nutzern aus, um Schadsoftware über infizierte Anhänge oder Links zu verbreiten oder digitale Identitäten für kriminelle Zwecke zu entwenden (BKA, 2011, 2018).

Cloud-Computing als Infrastruktur des Verbrechens

Cloud-Computing bietet Cyberkriminellen zweifache Nutzungsmöglichkeiten: Einerseits werden Cloud-Instanzen selbst zum Ziel von Angriffen, um massenhaft Datensätze zu exfiltrieren. Andererseits missbrauchen Täter Cloud-Server als leistungsstarke Plattformen, um von dort aus großvolumige Angriffe wie etwa DDoS-Attacken zu starten. Die schlechte Absicherung vieler Cloud-Konfigurationen stellt dabei ein persistentes Risiko für Unternehmen dar (BKA, 2019).

Die neue Ära durch Künstliche Intelligenz

Eine qualitative Änderung der Bedrohungslage markiert der Einsatz von KI. Spätestens seit der breiten Verfügbarkeit generativer KI-Modelle Ende 2022 nutzen Täter diese Werkzeuge, um Angriffe zu automatisieren und zu professionalisieren. KI ermöglicht die Erstellung authentischer Phishing-Nachrichten, die kaum noch von legitimer Kommunikation zu unterscheiden sind, und unterstützt Täter beim Schreiben oder Modifizieren von Malware-Codes (BKA, 2023, 2024, 2025; Honekamp & Kemme, 2025). Zudem senkt KI die Eintrittshürden für technisch weniger versierte Akteure, während erfahrene Gruppen ihre Fähigkeiten zur Analyse exfiltrierter Daten und zur Identifizierung von Schwachstellen weiter verstärken (BKA, 2023, 2024; Honekamp & Kemme, 2025). In der Underground Economy haben sich bereits spezifische kriminelle KI-Modelle wie WormGPT etabliert, die gezielt für die Begehung

von Straftaten entwickelt wurden (BKA, 2023, 2024). Technologische Innovationen haben das Deliktfeld Cybercrime kontinuierlich dynamisiert. Jede neue Stufe der Digitalisierung schafft zusätzliche Tatgelegenheitsstrukturen, die von einer anpassungsfähigen Täterseite zeitnah instrumentalisiert werden. Gleichzeitig eröffnet der Einsatz von KI auch für Strafverfolgungsbehörden neue Möglichkeiten, etwa bei der Mustererkennung in großen Datenbeständen, der Priorisierung von Ermittlungsansätzen oder der automatisierten Analyse digitaler Beweismittel. Der Einsatz solcher Systeme wirft jedoch zugleich erhebliche rechtliche und ethische Fragen auf (Honekamp, 2025).

Cybercrime als Querschnittsbedrohung

Im Verlauf der letzten Dekade hat sich Cybercrime von einem spezialisierten Randphänomen zu einer existenziellen Querschnittsbedrohung für Wirtschaft, Verwaltung und Gesellschaft entwickelt (BKA, 2019, 2024). Die fortschreitende Digitalisierung hat dazu geführt, dass Cyberangriffe heute weitreichende reale Konsequenzen nach sich ziehen können, die weit über den digitalen Raum hinausgehen (BKA, 2021, 2024).

Fokus auf Kritische Infrastrukturen und öffentliche Verwaltung

Kritische Infrastrukturen (KRITIS), wie die Sektoren Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur, erfüllen zentrale Versorgungs- und Steuerungsfunktionen moderner Gesellschaften und sind aufgrund ihrer herausgehobenen Bedeutung verstärkt in das Visier von Cyberkriminellen gerückt (BKA, 2018, 2019; BSI-KritisV). Bereits im Berichtsjahr 2016 dokumentierte das BKA eine Zunahme komplexer APT-Angriffe (Advanced Persistent Threat) auf KRITIS-Betreiber und staatliche Stellen wie den Deutschen Bundestag, wobei die Gefahr für die öffentliche Sicherheit durch die verstärkte Abhängigkeit der Produktion von vernetzten IuK-Technologien signifikant anstieg (BKA, 2017). Parallel dazu wurde die Dimension des industriellen Identitätsdiebstahls deutlich, als das BKA die „Anti Public Combo List“ mit ca. 500 Millionen kompromittierten Zugangsdaten identifizierte, die als Treiber für weitere zielgerichtete Angriffe in der Underground Economy dienten (BKA, 2017).

Ein KRITIS-Ausfall kann erhebliche Störungen der öffentlichen Sicherheit oder Versorgungsengpässe zur Folge haben (BKA, 2016, 2018). Besonders deutlich wurde diese Verwundbarkeit durch Angriffe auf Einrichtungen des Gesundheitswesens während der Pandemie sowie durch gezielte Ransomware-Attacken auf kommunale Verwaltungen. Ein prägnantes Beispiel hierfür bildet der im Juli 2021 im Landkreis Anhalt-Bitterfeld ausgerufene Katastrophenfall, der erstmals die realweltlichen Dimensionen digitaler Angriffe auf die staatliche Handlungsfähigkeit darlegte. Die Wiederherstellung der betroffenen Systeme nahm mehr als ein halbes Jahr in Anspruch und verursachte Kosten in Millionenhöhe (BKA, 2022).

Entwicklung zum Big Game Hunting

Die Täterstrategien haben sich weg von ungezielten Massenangriffen hin zum Big Game Hunting gewandelt. Dabei fokussieren sich professionelle Täterkollektive auf wirtschaftlich starke Unternehmen und Organisationen, um durch die Unterbrechung kritischer Geschäftsprozesse maximale Lösegeldforderungen durchzusetzen. Diese Angriffe sind oft gründlich vorbereitet und basieren auf einer detaillierten Informationssammlung über das Opfer. Ein wesentliches Element dieser Strategie ist der Modus Operandi der Double Extortion, bei dem die Verschlüsselung der Systeme mit der Drohung kombiniert wird, vorab exfiltrierte sensible Daten auf Leak-Websites im Darknet zu veröffentlichen. Dies erhöht den Druck auf die Opfer, da neben dem Betriebsausfall auch schwere Reputationsschäden drohen (BKA, 2020a, 2021, 2022, 2023, 2024, 2025). Die weitere Entwicklung zeigt, dass sich das Erpressungsmodell mehr und mehr ausdifferenziert. Für das Berichtsjahr 2025 weist das BKA 1.041 angezeigte Ransomware-Angriffe in Deutschland aus; in rund 76 % der Fälle konnte der Modus Operandi der Double Extortion festgestellt werden. Zugleich zahlten nach den vorliegenden Angaben nur 7 % der betroffenen Geschädigten Lösegeld, während die durchschnittlich gezahlten Beträge gegenüber dem Vorjahr deutlich anstiegen. Vor diesem Hintergrund gewinnt Data Extortion als eigenständiger Modus Operandi an Bedeutung, bei dem Täter auf die Verschlüsselung von Systemen verzichten und die Erpressung primär auf die Ausleitung und angedrohte Veröffentlichung sensibler Daten stützen. Diese Entwicklung veranschaulicht, dass die Täterstrategien vermehrt auf die ökonomische, rechtliche und reputative Verwundbarkeit der Opferorganisationen zielen (BKA, 2026).

Verzahnung mit geopolitischen Spannungsfeldern

Eine neue Qualität erreicht die Bedrohungslage durch die enge Verzahnung von Cybercrime mit geopolitischen Krisen. Insbesondere der russische Angriffskrieg gegen die Ukraine ab Februar 2022 hat gezeigt, dass der Cyberraum integraler Bestandteil moderner Konflikte ist (BKA, 2023). Neben staatlich gesteuerten Sabotageakten mittels destruktiver Malware (Wiper) treten verstärkt hacktivistische Akteure auf, die politisch motivierte DDoS-Kampagnen gegen Unterstützerstaaten führen. In diesem Kontext verschwimmen die Grenzen zwischen finanziell motivierter Kriminalität und politisch-ideologisch motivierten Angriffen zusehends. Tätergruppen nutzen dabei oft die gleichen technischen Werkzeuge und Infrastrukturen, unabhängig von ihrem eigentlichen Antrieb (BKA, 2023, 2025). Deutschland steht aufgrund seiner politischen und wirtschaftlichen Rolle im Zielspektrum hybrider Angriffskampagnen, die auf die Destabilisierung staatlicher und gesellschaftlicher Gefüge abzielen. Cybercrime stellt heute eine Bedrohung dar, die grundsätzlich jede Institution und jede Ebene des gesellschaftlichen Lebens treffen kann. Die Komplexität dieser Angriffe und die professionelle Organisation der Täterschaft machen Cybercrime zu einer dauerhaften Herausforderung für die nationale Sicherheit und die Resilienz des Wirtschaftsstandorts Deutschland (BKA, 2025).

Kontinuitäten und methodische Herausforderungen

Die Auswertung der Kriminalitätsentwicklung im digitalen Raum über zwei Jahrzehnte hinweg ergibt, dass neben den phänomenologischen Veränderungen auch die methodischen Rahmenbedingungen der polizeilichen Datenerhebung einer ständigen Evolution unterlagen. Diese Anpassungen waren notwendig, um der Dynamik des Feldes gerecht zu werden, erschweren jedoch gleichzeitig die langfristige Vergleichbarkeit quantitativer Daten (BKA, 2014, 2015, 2022).

Das persistente Problem des hohen Dunkelfelds

Ein zentrales Merkmal, das die gesamte Entwicklung von der Computerkriminalität zu Cybercrime begleitet, ist das weit überdurchschnittlich ausgeprägte Dunkelfeld. Polizeiliche Statistiken wie die PKS bilden lediglich das Hellfeld ab, also jene Taten, die polizeilich abschließend bearbeitet wurden (BKA, 2014, 2020a). Für den Bereich Cybercrime wird regelmäßig von einem erheblichen Dunkelfeld ausgegangen, weil Taten von Betroffenen nicht erkannt, aus Reputationsgründen nicht angezeigt oder erst bei ausbleibender Entschlüsselung nach einer Lösegeldzahlung zur Anzeige gebracht werden (BKA, 2010, 2021). Studien schätzen das Dunkelfeld im Bereich Cybercrime auf bis zu 91,5 % (BKA, 2022). Dabei hängen Hellfeld- und Dunkelfeldbefunde besonders stark von Definitionsentscheidungen, Anzeigeverhalten, Entdeckungswahrscheinlichkeit und Erhebungslogik ab. Bei Cybercrime-Statistiken und Hochrechnungen ist stets zu prüfen, wie Zahlen generiert werden, wie Täter und Opfer definiert sind, wie Schäden gemessen werden und ob es sich um Hellfeld- oder Dunkelfeldzahlen handelt. Veränderungen im polizeilichen Hellfeld dürfen daher nicht ohne Weiteres als proportionale Veränderungen der tatsächlichen Kriminalitätsbelastung interpretiert werden (Huber & Pospisil, 2020). Die Gründe hierfür sind vielfältig: Straftaten werden von den Betroffenen oft gar nicht erkannt, etwa bei unbemerkten Infektionen oder Identitätsdiebstahl (BKA, 2016, 2019). Huber und Pospisil (2020) verweisen in diesem Zusammenhang auf ein besonderes Dunkelfeldproblem bei Cybercrime: Delikte bleiben auch deshalb außerhalb der Statistik, weil Betroffene den Angriff selbst, den eingetretenen Schaden oder den strafrechtlichen Charakter des Geschehens nicht wahrnehmen. Das Dunkelfeld entsteht sowohl auf der Ebene fehlender Entdeckung als auch auf der Ebene fehlender Anzeige.

Eine ergänzende bevölkerungsbezogene Perspektive liefern Schwerthalter und Helmold (2026) im Cybersicherheitsmonitor. Die Befragung zeigt, dass 27 % der Befragten bereits mindestens einmal von Cyberkriminalität betroffen waren und 11 % eine entsprechende Straftat innerhalb der vergangenen zwölf Monate erlebt haben. Zugleich erstatteten nur 32 % der im Vorjahr Betroffenen Anzeige bei der Polizei. Diese Befunde sind methodisch nicht mit polizeilichen Hellfelddaten gleichzusetzen, da der Cybersicherheitsmonitor auf selbstberichteten Erfahrungen und Einstellungen beruht. Sie stützen jedoch die Annahme, dass polizeiliche Statistiken nur einen Ausschnitt der tatsächlichen Kriminalitätsbelastung abbilden und dass das Anzeigeverhalten eine zentrale Einflussgröße der Sichtbarkeit von Cybercrime bleibt.

Zudem verzichten insbesondere Unternehmen häufig aus Reputationsgründen auf eine Anzeige, um ihre Stellung als sicherer Partner im Markt nicht zu gefährden (BKA, 2013, 2018). Die begrenzte Sichtbarkeit von Cybercrime im Unternehmenskontext wird durch empirische Unternehmensbefragungen gestützt. Dreißigacker et al. (2023) zeigen auf Grundlage einer

zweiphasigen Befragung von 5.000 Unternehmen, dass Cyberangriffe im Unternehmenskontext weit verbreitet sind, aber nur begrenzt in Kontakt mit Strafverfolgungsbehörden gelangen. In der ersten Befragungsphase berichteten 41,1 % und in der zweiten Befragungsphase 59,6 % der Unternehmen von mindestens einem digitalen Angriff innerhalb der vorangegangenen zwölf Monate. Als häufige Angriffsformen traten insbesondere Phishing sowie Malware- und Ransomware-Angriffe hervor. Zugleich verdeutlichen die Befunde, dass Strafverfolgungsbehörden im Verhältnis zum tatsächlichen Tataufkommen nur eingeschränkt Zugang zu diesem Deliktsbereich erhalten, weil Unternehmen sie aufgrund geringer Anzeigebereitschaft häufig nicht als primäre Ansprechpartner wahrnehmen. In Erpressungsfällen erfolgt eine Anzeigeerstattung oft erst dann, wenn trotz einer Lösegeldzahlung die versprochene Entschlüsselung der Daten ausbleibt (BKA, 2015, 2020a).

Methodische Anpassungen und statistische Zäsuren

Um die Aussagekraft der Statistiken zu verbessern, wurden im betrachteten Zeitraum wesentliche methodische Änderungen vorgenommen. Eine gravierende Zäsur markiert das Jahr 2014 mit der bundeseinheitlichen Umstellung auf das Tatortprinzip. Seitdem werden Delikte im Bereich Cybercrime in der PKS grundsätzlich nur noch dann erfasst, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen (BKA, 2015, 2016). Dies führte dazu, dass die Zahlen vor 2014 keinen unmittelbaren Vergleichsmaßstab mehr für die Folgejahre bilden (BKA, 2015). Eine weitere bedeutende Entwicklung ist die zum 1. Januar 2020 eingeführte separate Erfassung von Auslandstaten (BKA, 2023, 2024). Da bei einem erheblichen Teil der Cybercrime-Fälle Schäden in Deutschland eintreten, der Aufenthaltsort der Tatverdächtigen jedoch unbekannt ist oder der Angriff aus dem Ausland heraus erfolgt, bildet die alleinige Betrachtung der Inlands-PKS die tatsächliche Bedrohungslage nur eingeschränkt ab. Für das Berichtsjahr 2025 weist das BKA 207.888 Auslandstaten und 126.034 Inlandstaten aus; in der zusammengefassten Betrachtung ergibt sich damit eine Gesamtzahl von 333.922 Cybercrime-Fällen. Die Auslandstaten übersteigen die Inlandstaten somit deutlich und verdeutlichen die zentrale Bedeutung einer erweiterten statistischen Betrachtung für die Bewertung der Cybercrime-Belastung in Deutschland (BKA, 2026). Im Jahr 2021 erfolgte zudem die Einführung eines neuen PKS-Summenschlüssels Cybercrime, der den bis dahin gebräuchlichen Schlüssel Computerkriminalität ersetzte und eine modernere, fachlich präzisere Beschreibung des Phänomens ermöglicht (BKA, 2022).

Grenzen der polizeilichen Statistik

Trotz dieser Weiterentwicklungen bleibt die PKS ein Hilfsmittel mit begrenzter Aussagekraft für die Gesamtkriminalität im digitalen Raum (BKA, 2010, 2017). Relevante Phänomene wie Phishing im Onlinebanking oder Erpressungen mittels DDoS-Attacken werden häufig unter den Schlüsseln der zugrunde liegenden Einzeltathandlungen, etwa der Erpressung, erfasst und tauchen somit statistisch nicht zwingend in der Kategorie Cybercrime im engeren Sinne auf (BKA, 2011, 2019). Zudem wird jede rechtswidrige Handlung unabhängig von der Anzahl der Opfer nur einmal erfasst, was bei massenhaft begangenen Delikten, wie der Manipulation von Millionen von Routern, zu einer extremen Diskrepanz zwischen der statistischen Fallzahl und der tatsächlichen Schadensdimension führt (BKA, 2016, 2017). Diese methodische Grenze wurde bereits in der frühen wissenschaftlichen Auseinandersetzung mit Computerkriminalität beschrieben.

Kempa (2006) weist darauf hin, dass die PKS die qualitative Unterschiedlichkeit digitaler Angriffe nur unzureichend sichtbar macht, weil ein Angriff auf einen privaten Einzelrechner und ein Angriff auf eine staatliche Einrichtung statistisch jeweils als ein Fall erscheinen können. Für die Bewertung von Cybercrime ist daher nicht allein die Häufigkeit registrierter Fälle relevant, sondern auch deren potenzielle Schadensreichweite, Systemrelevanz und infrastrukturelle Wirkung. Aus diesen Gründen betont das BKA regelmäßig, dass eine ganzheitliche Lagebewertung nur durch die Ergänzung des polizeilichen Hellfelds um qualitative Erkenntnisse aus dem Nachrichtenaustausch sowie um externe Quellen und Studien möglich ist (BKA, 2011, 2021).

Diese Erweiterung der Erkenntnisbasis verweist zugleich auf die Bedeutung institutionalisierter Kooperations- und Informationsaustauschstrukturen. Schwerthalter und Helmold (2026) verdeutlichen, dass diese Erweiterung nicht nur auf institutionelle Akteure beschränkt bleiben sollte. Auch das Informations- und Schutzverhalten der Bevölkerung bleibt für Prävention und Anzeigenaufkommen relevant: 2026 informierten sich nur 14 % der Befragten regelmäßig über Cybersicherheit, während 24 % angaben, sich eigentlich nie zu informieren. Von 19 vorgeschlagenen Schutzmaßnahmen wurden im Durchschnitt 3,9 genutzt; als Gründe für die Nichtnutzung nannten Befragte insbesondere ein hohes subjektives Sicherheitsgefühl, Komplexität und Überforderung.

Prävention, Detektion und Reaktion auf Cybercrime sind zunehmend auf kollaborative Ansätze zwischen Sicherheitsbehörden, Unternehmen und weiteren Akteuren der Cybersicherheitslandschaft angewiesen. Neben gesetzlichen Meldepflichten gewinnen freiwillige Austauschformate, Cyber-Security-Intelligence-Strukturen und vertrauensbasierte Kommunikationskanäle an Bedeutung, weil technische Indikatoren, Angriffsmuster und Erfahrungen aus konkreten Vorfällen häufig außerhalb des klassischen polizeilichen Hellfelds entstehen (Meywirth et al., 2023). Die Aussagekraft polizeilicher Erkenntnisse hängt darüber hinaus auch von der Qualität der ersten Informationsgewinnung ab. Gerade bei Cybercrime können bereits im Rahmen der Anzeigenaufnahme Hinweise auf mögliche Träger digitaler Spuren, auf Providerdaten oder auf zeitkritische Speicherfristen entscheidend sein, weil verspätet gesicherte oder unvollständig dokumentierte Daten spätere Ermittlungen erheblich erschweren können (Honekamp et al., 2020).

Schlussfolgerungen

Aus der polizeilichen Berichterstattung ergibt sich, dass sich Cybercrime im Verlauf des 21. Jahrhunderts von einer vorwiegend technisch verstandenen Deliktsgruppe zu einem eigenständigen, arbeitsteiligen und transnationalen Kriminalitätsfeld entwickelt hat. Entscheidend ist dabei weniger der terminologische Wechsel von Computerkriminalität zu Cybercrime als die veränderte analytische Perspektive: Digitale Kriminalität wird heute nicht mehr allein über einzelne Tatmittel oder manipulierte Systeme erfasst, sondern über Täterökosysteme, technische Infrastrukturen, Datenflüsse, Zahlungswege und internationale Verwertungszusammenhänge. Die Bundeslagebilder des BKA bilden diesen Perspektivwechsel seit 2010 empirisch ab und machen zugleich sichtbar, wie stark polizeiliche Lagebewertung von statistischen Erfassungslogiken, Dunkelfeldannahmen und ergänzenden externen Erkenntnisquellen abhängig bleibt.

Cybercrime hat sich zu einer strukturellen Querschnittsherausforderung entwickelt, die Wirtschaft, Verwaltung und Kritische Infrastrukturen gleichermaßen betrifft. Die erheblichen Schäden, die durch Ransomware-Kampagnen und Big Game Hunting verursacht werden können, unterstreichen die hohe Schadensrelevanz für Unternehmen, öffentliche Einrichtungen und den Wirtschaftsstandort Deutschland. Eine neue Qualität der Bedrohung ergibt sich zudem aus der engen Verzahnung mit geopolitischen Spannungsfeldern, wobei insbesondere der russische Angriffskrieg gegen die Ukraine den Cyberraum als integralen Bestandteil hybrider Konflikte etabliert hat. Für die Zukunft ist mit einer weiteren Verschärfung der Bedrohungslage zu rechnen. Technologische Multiplikatoren wie generative Künstliche Intelligenz werden die Effizienz und Authentizität von Angriffen, insbesondere im Bereich Phishing und Malware-Entwicklung, weiter steigern. Gleichzeitig bleibt das überdurchschnittlich hohe Dunkelfeld eine persistente Herausforderung für die polizeiliche Lagedarstellung und Kriminalitätsbekämpfung.

Die effektive Bekämpfung von Cybercrime erfordert deshalb eine Weiterentwicklung polizeilicher Technik, Organisation und Kooperationsstrukturen. Der Wandel der Täterseite zu arbeitsteiligen Dienstleistungs- und Infrastrukturmodellen lässt sich nicht allein mit klassischen, täterzentrierten Ermittlungsansätzen beantworten. Er verlangt eine polizeiliche Handlungsfähigkeit, die digitale Spuren frühzeitig erkennt, große Datenmengen strukturiert auswertet, technische Infrastrukturen analysiert, Zahlungsströme nachvollzieht und Erkenntnisse über Zuständigkeits- und Ländergrenzen hinweg bündelt. Dadurch wird Cybercrime-Bekämpfung zu einer Querschnittsaufgabe, die spezialisierte Cybercrime-Dienststellen ebenso betrifft wie die Fähigkeit der Fläche, erste digitale Spuren sachgerecht zu sichern und spätere gerichtsverwertbare Auswertungen nicht durch frühe Verfahrensfehler zu gefährden. Zugleich bleibt polizeiliches Handeln im Cyberraum rechtlich und praktisch begrenzt: Maßnahmen gegen Täterinfrastrukturen, internationale Datenerhebungen und operative Eingriffe in verteilte Systeme setzen klare Zuständigkeiten, belastbare Kooperationsmechanismen und eine realistische Einschätzung technischer Umsetzbarkeit voraus. Cybercrime bleibt eine dynamische Dauerherausforderung, deren Bewältigung nicht in einer einmaligen technischen Anpassung besteht, sondern in der fortlaufenden Fähigkeit, polizeiliche Analyse-, Ermittlungs- und Kooperationsstrukturen an die Dynamik digitaler Täterökosysteme anzupassen.

Referenzen

Atug, M. (2023). Ransomware als Business Case in der organisierten Kriminalität. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2: Phänomene und Auswirkungen (S. 345–383). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_38

BKA. (2002). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2001. Bundeskriminalamt.

BKA. (2003). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2002. Bundeskriminalamt.

BKA. (2004). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2003. Bundeskriminalamt.

BKA. (2005). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2004. Bundeskriminalamt.

BKA. (2006). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2005. Bundeskriminalamt.

BKA. (2009). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2008. Bundeskriminalamt.

BKA. (2010). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 2009. Bundeskriminalamt.

BKA. (2011). Cybercrime Bundeslagebild 2010. Bundeskriminalamt.

BKA. (2012). Cybercrime Bundeslagebild 2011. Bundeskriminalamt.

BKA. (2013). Cybercrime Bundeslagebild 2012. Bundeskriminalamt.

BKA. (2014). Cybercrime Bundeslagebild 2013. Bundeskriminalamt.

BKA. (2015). Cybercrime Bundeslagebild 2014. Bundeskriminalamt.

BKA. (2016). Cybercrime Bundeslagebild 2015. Bundeskriminalamt.

BKA. (2017). Cybercrime Bundeslagebild 2016. Bundeskriminalamt.

BKA. (2018). Cybercrime Bundeslagebild 2017. Bundeskriminalamt.

BKA. (2019). Cybercrime Bundeslagebild 2018. Bundeskriminalamt.

BKA. (2020a). Cybercrime Bundeslagebild 2019. Bundeskriminalamt.

BKA. (2020b). Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie. Bundeskriminalamt.

BKA. (2021). Cybercrime Bundeslagebild 2020. Bundeskriminalamt.

BKA. (2022). Cybercrime Bundeslagebild 2021. Bundeskriminalamt.

BKA. (2023). Cybercrime Bundeslagebild 2022. Bundeskriminalamt.

BKA. (2024). Cybercrime Bundeslagebild 2023. Bundeskriminalamt.

BKA. (2025). Cybercrime Bundeslagebild 2024. Bundeskriminalamt.

BKA. (2026). Cybercrime Bundeslagebild 2025. Bundeskriminalamt.

Bundesregierung. (2026). Entwurf eines Gesetzes zur Stärkung der Cybersicherheit. https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/cyberabwehr-regierungsentwurf.pdf

Dewald, A., & Freiling, F. C. (2015). Forensische Informatik. BoD.

Dreißigacker, A., von Skarczinski, B. S., & Wollinger, G. R. (2023). Unternehmen als Opfer von Cyberkriminalität. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2: Phänomene und Auswirkungen (S. 587–609). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_43

Honekamp, W. (2025). Die Auswirkungen Künstlicher Intelligenz auf die Polizeiarbeit. Deutsches Polizeiblatt. 43(6), 15–18.

Honekamp, W., & Kemme, S. (2025). Herausforderungen für die Arbeit der Polizei durch den Einsatz von KI auf Täter:innenseite – technische und kriminologische Erkenntnisse am Beispiel großer Sprachmodelle. In W. Honekamp, S. Kemme & J. Struck (Hrsg.), Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 347–372). Springer Gabler. https://doi.org/10.1007/978-3-658-48425-5_20

Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., & Labudde, D. (2023). Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2. Phänomene und Auswirkungen (S. 673–702). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_51

Honekamp, W., Povalej, R., Rittelmeier, H., & Labudde, D. (2020). Bekämpfung von Cybercrime durch die Polizei. In G. R. Wollinger & A. Schulze (Hrsg.), Handbuch Cybersecurity für die öffentliche Verwaltung (S. 111–138). Kommunal- und Schul-Verlag. https://doi.org/10.5771/9783748912057

Huber, E., & Pospisil, B. (2020). Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Cyberkriminologie: Kriminologie für das digitale Zeitalter (S. 109–133). Springer VS. https://doi.org/10.1007/978-3-658-28507-4_4

Kempa, D. (2006). Angriff auf Netze und Systeme: Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung. Dissertation, Universität Hamburg. https://ediss.sub.uni-hamburg.de/handle/ediss/1462

Kunze, D. (2023). Bearbeitung von Cyberangriffen unter Berücksichtigung der polizeilichen Vorschriftenlage und fachliche, technische und rechtliche Determinanten erfolgreicher Cyberoperationen gegen angreifende Infrastrukturen und Tätergruppierungen (Hack Back). In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 1: Theorien und Methoden (S. 543–574). Springer VS. https://doi.org/10.1007/978-3-658-35439-8_22

Meywirth, C., Pauker, A., & Sowa, A. (2023). Cybercrime und Cyber Security Intelligence: Kollaborative Ansätze gegen Cyber- und Computerkriminalität. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 2: Phänomene und Auswirkungen (S. 731–754). Springer VS. https://doi.org/10.1007/978-3-658-35442-8_54

Plank, H. (2020). Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Cyberkriminologie: Kriminologie für das digitale Zeitalter (S. 13–70). Springer VS. https://doi.org/10.1007/978-3-658-28507-4_2

Plank, H., & Fiedler, A. (2023). Das „Spuren- und Indizienparadigma“ – Bedeutung innerhalb von Cyberkriminalistiken. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), Handbuch Cyberkriminologie 1: Theorien und Methoden (S. 71–136). Springer VS. https://doi.org/10.1007/978-3-658-35439-8_3

Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., Honekamp, W., & Labudde, D. (2021). Die Enkel von Locard. Informatik Spektrum 44, 355–363. https://doi.org/10.1007/s00287-021-01393-5

Schwerthalter, B. & Helmold, D. (2026). Befragung zur Cybersicherheit 2026: Kurzbericht zur Studie der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Bundesamt für Sicherheit in der Informationstechnik; Polizeiliche Kriminalprävention der Länder und des Bundes. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html

Siegert, M. (2002). Das Internet – Grundlagenwissen für die Polizei: Geschichte, Technik, Multimediarecht, Strafrecht, Strafprozeßrecht, Gefahrenabwehr, Kinderpornographie. TENEA. https://jurawelt.com/sunrise/media/mediafiles/13817/tenea_juraweltbd20.pdf

Polizeihochschulen als Schnittstellen technischer Transformation

Johannes Fähndrich und Wilfried Honekamp

Polizeiliche Technikentwicklung ist im 21. Jahrhundert nicht mehr auf einzelne Einsatzmittel oder isolierte Fachverfahren beschränkt. Digitale Akten, automatisierte Auswertungssysteme, mobile Endgeräte, Kommunikationsplattformen, digitale Spurensicherung, biometrische Verfahren und KI-gestützte Anwendungen verändern Arbeitsabläufe, Zuständigkeiten und Kompetenzanforderungen innerhalb der Polizei. Neue Technik muss nicht nur beschafft und eingeführt werden. Sie muss fachlich geprüft, rechtlich eingeordnet, organisatorisch eingebettet, technisch betrieben und in Aus- und Fortbildung vermittelt werden. Damit wird technologische Handlungsfähigkeit zu einer Ausbildungs- und Organisationsfrage. Gerade große Polizeiorganisationen stehen vor der Herausforderung, mit der Geschwindigkeit technischer Entwicklungen Schritt zu halten, ohne Anforderungen an Rechtssicherheit, Praxistauglichkeit und professionelle Handlungskompetenz zu vernachlässigen.

Der Beitrag untersucht diese Frage nicht als allgemeine hochschulpolitische Strukturkritik, sondern mit Blick auf die Bedingungen polizeitechnischer Handlungsfähigkeit. Im Mittelpunkt steht die These, dass eine technologische Entkopplung entstehen kann, wenn die polizeiliche Einsatz- und Ermittlungsrealität schneller technisiert wird, als Ausbildung, Forschungskapazität und curriculare Entwicklung darauf reagieren. Analysiert werden daher drei miteinander verbundene Aspekte: die Dynamik polizeilicher Technikentwicklung, die curricularen und rechtlichen Anforderungen an den Umgang mit KI und digitalen Technologien sowie die institutionellen Voraussetzungen, unter denen Polizeihochschulen technisches Wissen aufnehmen, bewerten und in Ausbildung überführen können.

Polizeitechnische Handlungsfähigkeit als Ausbildungsaufgabe

Polizeitechnik entfaltet ihre Wirkung nicht allein durch Verfügbarkeit, Beschaffung oder technische Leistungsfähigkeit. Entscheidend ist, ob technische Systeme in polizeiliche Arbeitsprozesse sachgerecht eingebettet, rechtlich zulässig genutzt und von den Anwenderinnen und Anwendern professionell beherrscht werden. Dies gilt in besonderem Maße für digitale und datenbasierte Technologien. Automatisierte Auswertungssysteme, KI-gestützte Analysen, digitale Spurensicherung, biometrische Verfahren, Drohnentechnik und mobile Informationssysteme verändern nicht nur einzelne Arbeitsmittel der Polizei. Sie verändern auch Anforderungen an Ausbildung, Fortbildung, Dokumentation, Fehlerbewertung und institutionelle Wissensverarbeitung. Die Forschung zur Technologiewirkung in der Polizei weist darauf hin, dass technische Innovationen ihre Wirkung nicht automatisch entfalten. Koper et al. (2014, 2015) zeigen, dass die erfolgreiche Implementierung polizeilicher Technologien wesentlich von sozialen, organisationalen und verhaltensbezogenen Bedingungen abhängt. Lum et al. (2017) weisen zudem darauf hin, dass der Nutzen neuer Polizeitechnologien häufig überschätzt wird, wenn ihre Einführung nicht durch Forschung, Evaluation und Ausbildung begleitet wird. Polizeitechnik ist damit auch eine Frage institutioneller Übersetzungsfähigkeit.

Für die Polizeiausbildung folgt daraus, dass technische Bedienkompetenz allein nicht ausreicht. Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte müssen einschätzen können, welche Daten ein System verarbeitet, welche Aussagekraft technische Ergebnisse besitzen, welche Fehlerquellen bestehen, welche Dokumentationspflichten zu beachten und wann rechtliche oder fachliche Grenzen erreicht sind. Honekamp et al. (2023) zeigen dies am Beispiel digitaler Spuren: Schon bei einem inzwischen etablierten Technologiebereich bestehen Anforderungen, die über einfache Anwendungsschulung hinausgehen und technische, kriminalistische, rechtliche und methodische Kompetenzen miteinander verbinden. Diese Entwicklung zeigt sich unter anderem beim Einsatz Künstlicher Intelligenz. Das Positionspapier des Bitkom-Arbeitskreises Sicherheitsbehörden beschreibt KI als ein Handlungsfeld, in dem Wissenslücken, Skepsis und fehlende Anwendungssicherheit die behördliche Technologieadoption hemmen können (Bitkom e. V., 2023). Auch die BKA-Herbsttagung 2024 verdeutlichte, dass KI nicht mehr nur als Zukunftstechnologie zu behandeln ist, sondern bereits polizeiliche Arbeitsprozesse, Analysefähigkeiten und Formen kriminellen Missbrauchs beeinflusst (Bundeskriminalamt, 2024). Damit verschärft sich die Ausbildungsfrage: Wer KI-gestützte Systeme polizeilich nutzt, muss deren Ergebnisse einordnen, ihre Grenzen erkennen und ihre Anwendung rechtlich verantworten können.

Polizeihochschulen nehmen in diesem Zusammenhang eine Vermittlungsfunktion ein. Sie stehen zwischen polizeilicher Praxis, technologischer Entwicklung, rechtlicher Regulierung und wissenschaftlicher Reflexion. Internationale Arbeiten zur Polizeitechnologie betonen deshalb zunehmend die Rolle von Ausbildungs- und Forschungseinrichtungen als Technologiemittler. Der Policy Toolkit der Police Foundation/PERIL (2024) sowie der PESTT-Bericht des Police Science and Technology Advisory Council und des UK Home Office (2024) verweisen darauf, dass neue Polizeitechnologien frühzeitig beobachtet, bewertet und in Organisations- sowie Ausbildungsprozesse übersetzt werden müssen. Für Polizeihochschulen bedeutet dies, dass sie nicht nur bestehende Praxis abbilden, sondern technologische Entwicklungen fachlich einordnen und curricular verarbeiten müssen. Die Hochschule für Polizei Baden-Württemberg dient dem Beitrag hierfür als exemplarischer Bezugspunkt. Sie bildet die Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten des Landes aus und ist zugleich mit anwendungsorientierter Forschung beauftragt. Dadurch bündelt sie zwei Funktionen, die für den Umgang mit moderner Polizeitechnik relevant sind: die Vermittlung berufspraktischer Kompetenz und die wissenschaftliche Reflexion technischer, rechtlicher und organisatorischer Entwicklungen. Gerade an dieser Schnittstelle stellt sich die Frage, ob bestehende Ausbildungsstrukturen ausreichen, um technologische Dynamik, rechtliche Komplexität und praktische Anwendungssicherheit angemessen miteinander zu verbinden.

Methodisches Vorgehen und Materialgrundlage

Der Beitrag ist als konzeptionell ausgerichtete Literaturübersicht angelegt. Im Mittelpunkt steht die Frage, unter welchen Bedingungen Polizeihochschulen technologische Entwicklungen aufnehmen, bewerten und in Ausbildung überführen können. Die Analyse verbindet Forschung zu Polizeitechnologie, Technologieadoption und evidenzbasierter Polizeiarbeit mit Literatur zu polizeilicher Ausbildung, KI-Governance und digitaler Transformation. Die Literaturrecherche folgte einem strukturierten Ansatz. Als Ausgangsbasis dienten einschlägige Datenbanken und Repositorien, darunter SSOAR, Google Scholar, POLINFO, Veröffentlichun-

gen der Deutschen Hochschule der Polizei, der HSPV NRW, der Hochschule für Polizei Baden-Württemberg sowie europäische polizeiwissenschaftliche Publikationskontexte wie das CEPOL Research Bulletin. Ergänzend wurden praxisnahe und institutionelle Quellen berücksichtigt. Dazu zählen Positionspapiere der Hochschulverbände, Jahresberichte polizeilicher Forschungsinstitute sowie Studien und Berichte zu Technologieeinsatz, Digitalisierung und KI-Governance in Sicherheitsbehörden. Einbezogen wurden Publikationen bis einschließlich Frühjahr 2026. Die Auswahl der Quellen orientierte sich an ihrer Relevanz für drei Analysebereiche: erstens die Dynamik polizeilicher Technikentwicklung, zweitens die curricularen und rechtlichen Anforderungen an den Umgang mit digitalen und KI-gestützten Technologien, drittens die institutionellen Voraussetzungen polizeitechnischer Handlungsfähigkeit.

Analysebefunde zur polizeitechnischen Entkopplung

Die ausgewerteten Quellen weisen darauf hin, dass polizeiliche Technikentwicklung und polizeiliche Ausbildung unterschiedlichen Veränderungslogiken folgen. Während digitale und datenbasierte Technologien in immer kürzeren Innovationszyklen in die polizeiliche Praxis gelangen, sind Studienordnungen, Curricula und Lehrformate auf längere Planungs- und Anpassungszeiträume ausgerichtet. Daraus ergibt sich eine strukturelle Spannung zwischen technischer Einsatzrealität und curricularer Verarbeitung. Ein erster Befund betrifft die Breite und Dynamik der technischen Entwicklung. Polizeiliche Praxis ist inzwischen nicht mehr nur durch einzelne technische Hilfsmittel geprägt. Sie umfasst ein breites Spektrum digitaler und physischer Technologien, darunter automatische Kennzeichenerkennung, KI-gestützte Videoauswertung, Drohnen, biometrische Erkennungssysteme, digitale Spurensicherungstechnik und LLM-basierte Assistenzsysteme für kriminalanalytische Zwecke. Diese Entwicklung wird auch in aktuellen polizeitechnischen Übersichten und Lageeinschätzungen sichtbar, die auf eine zunehmende Bedeutung von KI-Anwendungen, datenbasierten Analyseverfahren, Deepfake-Erkennung, digitaler Forensik und technologiegestützter Lageauswertung verweisen (Honekamp & Klingelhöfer, 2025; INTERPOL Innovation Centre, 2026; Police Science and Technology Advisory Council / UK Home Office, 2024). Die genannten Technologien unterscheiden sich hinsichtlich Funktionsweise, Eingriffstiefe, Fehleranfälligkeit, Dokumentationsbedarf und rechtlicher Steuerung. Für die Ausbildung bedeutet dies, dass technisches Wissen nicht als isoliertes Spezialwissen einzelner Fachgebiete behandelt werden sollte. Es muss vielmehr in unterschiedlichen Lehrbereichen anschlussfähig werden, etwa in Kriminalistik, Eingriffsrecht, Ethik, Datenschutz, Einsatzlehre und digitaler Beweissicherung.

Ein zweiter Befund betrifft die rechtliche und methodische Komplexität technischer Anwendungen. Der Einsatz KI-gestützter Systeme, digitaler Spurensicherung und datenbasierter Analyseverfahren setzt nicht nur Bedienkompetenz voraus. Er verlangt auch die Fähigkeit, technische Ergebnisse hinsichtlich Aussagekraft, Fehlerquellen, Datenqualität, Nachvollziehbarkeit und rechtlicher Zulässigkeit einzuordnen. Dies gilt insbesondere für Systeme, die personenbezogene Daten verarbeiten, biometrische Merkmale auswerten, Risikoeinschätzungen unterstützen oder polizeiliche Priorisierungen beeinflussen. Die Literatur zur digitalen Spurensicherung zeigt, dass bereits etablierte Technologiebereiche erhebliche Anforderungen an technische, kriminalistische, rechtliche und methodische Kompetenzen stellen. Für KI-gestützte Anwendungen verdichten sich diese Anforderungen zusätzlich. Ein dritter Befund betrifft die institutionelle Vermittlungsfunktion von Polizeihochschulen. Die

Forschung zur Technologieadoption in der Polizei zeigt, dass der Nutzen neuer Technik nicht allein von ihrer technischen Leistungsfähigkeit abhängt. Entscheidend sind auch Organisation, Ausbildung, Akzeptanz, Fehlerlernen und die Fähigkeit, technische Neuerungen in professionelle Routinen zu übersetzen. Polizeihochschulen nehmen dabei eine Zwischenstellung ein: Sie müssen polizeiliche Praxisanforderungen aufnehmen, technologische Entwicklungen beobachten, rechtliche Anforderungen berücksichtigen und daraus vermittelbare Ausbildungsinhalte entwickeln. Wenn diese Übersetzungsleistung nicht gelingt, entsteht eine Lücke zwischen Technikeinsatz und Handlungssicherheit.

Diese Vermittlungsfunktion hängt nicht nur von curricularen Entscheidungen ab, sondern auch von den institutionellen Voraussetzungen, unter denen Forschung und Lehre an Polizeihochschulen verbunden werden können. Die in der Literatur beschriebenen Strukturen der Hochschulen für den öffentlichen Dienst verweisen auf begrenzte wissenschaftliche Personalkapazitäten, hohe Lehrverpflichtungen und eine häufig schwach ausgeprägte Mittelbaustruktur (Hochschullehrerbund hlb, 2025; Rektorenkonferenz der Hochschulen für den öffentlichen Dienst, 2023). Für die polizeitechnische Ausbildung ist dies relevant, weil technische Entwicklungen kontinuierlich beobachtet, fachlich bewertet und in Lehrinhalte übersetzt werden müssen. Wo hierfür keine stabilen Forschungs- und Transferstrukturen bestehen, bleibt die curriculare Verarbeitung neuer Technologien stärker von einzelnen Personen, zeitlich befristeten Initiativen oder externen Impulsen abhängig.

Ein vierter Befund betrifft die infrastrukturellen Voraussetzungen polizeitechnischer Ausbildung. Technische Entwicklungen können nicht allein über curriculare Anpassungen verarbeitet werden. Sie setzen auch Lehr- und Lernumgebungen voraus, in denen digitale Fallarbeit, simulationsbezogene Übungsformate, die Analyse technischer Fehlerquellen und die reflektierte Anwendung datenbasierter Systeme didaktisch abgebildet werden können. Technologische Entkopplung ist daher nicht nur als Inhaltsproblem zu verstehen. Sie betrifft auch die Frage, ob Ausbildungsinstitutionen über räumliche, technische und organisatorische Bedingungen verfügen, die eine praxisnahe und zugleich methodisch kontrollierte Vermittlung neuer Technologien ermöglichen.

Polizeihochschulen als Schnittstellen polizeitechnischer Transformation

Die Analyse ergibt, dass sich polizeiliche Technikentwicklung und Ausbildungsstrukturen nicht im gleichen Tempo verändern. Das Problem liegt daher nicht nur darin, ob einzelne neue Technologien bereits in Lehrveranstaltungen vorkommen. Entscheidend ist vielmehr, ob Polizeihochschulen technische Entwicklungen früh genug beobachten, rechtlich und methodisch einordnen und so aufbereiten können, dass daraus belastbare Ausbildungsinhalte entstehen. Polizeitechnische Handlungsfähigkeit entsteht nicht schon dadurch, dass neue Systeme in der Praxis eingeführt werden. Sie setzt voraus, dass Ausbildungseinrichtungen diese Entwicklungen aufnehmen, bewerten und in konkrete Kompetenzen für den polizeilichen Alltag überführen. Die Analyse schließt an die in der Forschung zur Technologieadoption in der Polizei beschriebene Annahme an, dass Polizeitechnik ihre Wirkung nicht allein aus technischer Verfügbarkeit oder Leistungsfähigkeit entfaltet. Koper et al. (2014, 2015) zeigen, dass die erfolgreiche Implementierung polizeilicher Technologien wesentlich von sozialen, organisationalen und verhaltensbezogenen Bedingungen abhängt. Lum et al.

(2017) weisen ergänzend darauf hin, dass neue Polizeitechnik in ihrer Wirkung überschätzt werden kann, wenn Einführung, Evaluation und Ausbildung nicht systematisch miteinander verbunden werden. Vor diesem Hintergrund ist technologische Entkopplung nicht lediglich als Randproblem der Lehre zu verstehen. Sie betrifft die Frage, ob technische Innovationen in polizeiliche Handlungskompetenz überführt werden können. Die Ergebnisse verdeutlichen, dass Polizeihochschulen dabei eine Übersetzungsfunktion übernehmen. Sie müssen technische Entwicklungen nicht selbst hervorbringen, aber sie müssen deren polizeiliche Relevanz, rechtliche Grenzen und methodische Voraussetzungen in Ausbildung übersetzen. Dies entspricht der von der Police Foundation/PERIL (2024) beschriebenen Rolle polizeilicher Bildungs- und Forschungseinrichtungen als Vermittlungsinstanzen zwischen technischer Innovation, organisationaler Implementierung und professioneller Praxis. Auch der PESTT-Bericht des Police Science and Technology Advisory Council und des UK Home Office (2024) verweist auf die Notwendigkeit, technische Entwicklungen frühzeitig zu beobachten und ihre Bedeutung für polizeiliche Organisationen systematisch zu bewerten. Für Polizeihochschulen folgt daraus, dass sie nicht erst reagieren können, wenn eine Technologie flächendeckend eingeführt ist. Sie müssen bereits vorher Kompetenzen aufbauen, die einen sachgerechten, rechtssicheren und reflektierten Umgang ermöglichen.

Dazu gehört auch, technische Implementierungen nicht nur als Erfolgsgeschichten zu behandeln. Die Forschung zu Innovation und organisationalem Lernen weist darauf hin, dass neue Verfahren vor allem dann nachhaltig in Organisationen aufgenommen werden können, wenn auch Unsicherheiten, Fehlannahmen und nicht intendierte Folgen bearbeitet werden. Für die Polizeiausbildung bedeutet dies, dass Studierende nicht nur mit Funktionsweisen neuer Technologien vertraut gemacht werden sollten. Ebenso wichtig ist die didaktische Auseinandersetzung mit fehlerhaften Anwendungen, begrenzter Datenqualität, unklaren Zuständigkeiten und Situationen, in denen technische Ergebnisse falsch interpretiert oder organisatorisch überschätzt werden (Kriegesmann et al., 2007; Ordon et al., 2019; Sun et al., 2025).

Dies zeigt sich auch bei KI-gestützten Anwendungen. Das Positionspapier des Bitkom-Arbeitskreises Sicherheitsbehörden beschreibt Wissenslücken, Skepsis und fehlende Anwendungssicherheit als Hemmnisse der Technologieadoption in Sicherheitsbehörden (Bitkom e. V., 2023). Die BKA-Herbsttagung 2024 ordnet KI ebenfalls als bereits praxisrelevanten Faktor polizeilicher Arbeit ein (Bundeskriminalamt, 2024). Die vorliegenden Analysebefunde schließen hieran an: Wenn KI-Systeme polizeiliche Analyse-, Bewertungs- oder Priorisierungsprozesse unterstützen, entstehen Ausbildungsanforderungen, die über Bedienwissen hinausgehen. Erforderlich sind Grundkenntnisse zu Datenqualität, Modellgrenzen, Fehleranfälligkeit, Transparenz, menschlicher Verantwortung und rechtlicher Zulässigkeit. Ohne solche Kompetenzen kann KI zwar technisch eingesetzt werden, bleibt aber professionell und rechtsstaatlich nur eingeschränkt beherrschbar. Die Diskussion um digitale Spuren zeigt, dass dieses Problem nicht erst mit KI beginnt. Honekamp et al. (2023) machen am Beispiel technologiegetriebener Polizeiausbildung im Umgang mit digitalen Spuren deutlich, dass technische, kriminalistische, rechtliche und methodische Anforderungen bereits in etablierten Technologiebereichen eng miteinander verbunden sind. Digitale Beweismittel müssen nicht nur gefunden und gesichert werden. Ihre Erhebung, Verarbeitung und Interpretation müssen nachvollziehbar, dokumentiert und rechtlich verwertbar bleiben. Die Ergebnisse

des vorliegenden Beitrags knüpfen an diesen Befund an: Wenn digitale Spurensicherung curriculare Anforderungen erzeugt, gilt dies auch für KI-gestützte Analysen, biometrische Verfahren, automatisierte Videoauswertung oder LLM-basierte Assistenzsysteme.

Damit lässt sich der Blick auf Polizeitechnik erweitern. Sie erscheint nicht mehr allein als Gegenstand von Beschaffung, Fachverfahren oder operativer Anwendung. Polizeitechnik wird zu einem Gegenstand professioneller Kompetenzbildung. Diese Kompetenz umfasst technisches Grundverständnis, rechtliche Einordnung, methodische Bewertung, Sensibilität für Fehlerquellen und die Fähigkeit, technische Ergebnisse in polizeiliche Entscheidungen einzubetten. Lum und Koper (2015) sowie Lum et al. (2017) betonen, dass der tatsächliche Nutzen polizeilicher Technologien empirisch geprüft und nicht vorausgesetzt werden sollte. Für die Ausbildung bedeutet dies, dass neue Technik nicht nur als Modernisierungsversprechen vermittelt werden darf. Sie muss auch hinsichtlich Wirksamkeit, Grenzen und unbeabsichtigter Folgen thematisiert werden. Der Blick auf die HfPolBW als exemplarischen Bezugspunkt lässt sich in diesem Zusammenhang als Hinweis auf ein breiteres Strukturproblem lesen. Die Hochschule steht für eine Ausbildungsinstitution, die berufspraktische Qualifizierung, anwendungsorientierte Forschung und curriculare Entwicklung miteinander verbinden soll. Diese Verbindung ist für den Umgang mit moderner Polizeitechnik bedeutsam. Wenn Forschungskapazitäten, curriculare Anpassungsprozesse und Lehrinfrastrukturen nicht Schritt halten, entsteht eine Lücke zwischen technischer Entwicklung und Ausbildungspraxis. Diese Lücke betrifft nicht nur einzelne Lehrinhalte. Sie betrifft auch die Fähigkeit der Institution, technologische Entwicklungen zu beobachten, ihre polizeiliche Relevanz zu bewerten und daraus belastbare Lehrformate zu entwickeln.

Dass diese institutionellen Voraussetzungen unterschiedlich ausgeprägt sein können, zeigt der Blick auf andere polizeiliche Hochschul- und Forschungskontexte. Die Deutsche Hochschule der Polizei, das Institut für Polizei- und Kriminalwissenschaften an der HSPV NRW oder das Sächsische Institut für Polizei- und Sicherheitsforschung stehen beispielhaft für stärker institutionalisierte Formen polizeibezogener Forschung und Wissensverarbeitung (Deutsche Hochschule der Polizei, 2026; Ruch et al., 2025; Sächsisches Institut für Polizei- und Sicherheitsforschung, 2024). Für den vorliegenden Beitrag ist dieser Vergleich nicht als Ranking von Einrichtungen relevant. Er verdeutlicht vielmehr, dass polizeitechnische Handlungsfähigkeit auch davon abhängt, ob Hochschulen über dauerhafte Strukturen verfügen, in denen technische Entwicklungen beobachtet, wissenschaftlich eingeordnet und in Ausbildungskontexte übersetzt werden können.

Die von Police Foundation/PERIL (2024) und dem PESTT-Bericht des Police Science and Technology Advisory Council und des UK Home Office (2024) angesprochene Funktion des Technologiemonitorings gewinnt vor diesem Hintergrund an Bedeutung. Polizeihochschulen sollten nicht jede technische Entwicklung unmittelbar curricular abbilden. Sie benötigen jedoch Verfahren, um relevante Entwicklungen frühzeitig zu identifizieren, ihre polizeiliche Bedeutung einzuschätzen und priorisierte Kompetenzanforderungen abzuleiten. Dies betrifft etwa KI-gestützte Analysewerkzeuge, digitale Spurensicherung, Drohnenabwehr, biometrische Verfahren, Deepfake-Erkennung und datenbasierte Lagebilder. Fehlt eine solche Beobachtungs- und Bewertungsfunktion, kann das Risiko steigen, dass Ausbildung technischen Entwicklungen nur verzögert folgt.

Daraus ergibt sich eine enger auf Polizeitechnik bezogene Schlussfolgerung: Institutionelle Fragen wie Forschungskapazität, Vernetzung, Lehrinfrastruktur und curriculare Steuerung sind nicht wegen einer abstrakten Akademisierungsdebatte relevant. Sie sind relevant, weil sie darüber entscheiden, ob polizeitechnisches Wissen rechtzeitig aufgenommen, geprüft und professionsbezogen vermittelt werden kann. Koper et al. (2014, 2015), Lum et al. (2017), Honekamp et al. (2023), Bitkom e. V. (2023), Bundeskriminalamt (2024), Police Foundation/PERIL (2024) und der PESTT-Bericht des Police Science and Technology Advisory Council und des UK Home Office (2024) verweisen aus unterschiedlichen Perspektiven auf denselben Zusammenhang: Technikadoption in der Polizei hängt nicht von Technik allein ab. Sie benötigt Organisation, Ausbildung, Evaluation, rechtliche Einordnung und reflektierte Anwendung.

Ausbildung als Bestandteil polizeitechnischer Infrastruktur

Für die Entwicklung der Polizeitechnik im 21. Jahrhundert bedeutet dies, dass Ausbildung selbst als Teil polizeitechnischer Infrastruktur verstanden werden muss. Technische Systeme werden polizeilich nicht allein dadurch wirksam, dass sie beschafft oder in der Praxis verfügbar gemacht werden. Sie müssen verstanden, eingeordnet, begrenzt und verantwortungsvoll eingesetzt werden können. Polizeihochschulen tragen dazu bei, diese Voraussetzungen herzustellen. Ihre Aufgabe besteht nicht nur darin, bestehende Techniknutzung nachträglich in Lehrveranstaltungen abzubilden. Sie müssen technische Entwicklungen beobachten, ihre polizeiliche Relevanz bewerten, rechtliche und methodische Grenzen sichtbar machen und daraus belastbare Ausbildungsinhalte entwickeln. Dafür benötigen sie curriculare Anpassungsfähigkeit, geeignete Lehrinfrastrukturen, Forschungskapazitäten und Verfahren des Technologiemonitorings. Der Beitrag zeigt damit, dass die Entwicklung der Polizeitechnik auch eine Frage der institutionellen Fähigkeit ist, technisches Wissen in professionelle Handlungskompetenz zu überführen. Wo diese Übersetzungsleistung gelingt, kann Ausbildung dazu beitragen, technische Innovationen rechtsstaatlich, methodisch reflektiert und praxistauglich in polizeiliches Handeln zu integrieren.

Referenzen

Bitkom e. V. (2023). *KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung*. https://www.bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf

Bundeskriminalamt. (2024). *Auf der Spur mit KI – wie KI die polizeiliche Welt revolutioniert. Tagungsbroschüre Herbsttagung 2024*.

Deutsche Hochschule der Polizei. (2026). Tätigkeitsbericht 2025. Deutsche Hochschule der Polizei. https://www.dhpol.de/berichte_und_bekanntmachungen/Taetigkeitsbericht_2025_final.pdf

Hochschullehrerbund hlb. (2025). Hochschulen für den öffentlichen Dienst stärken! Positionspapier. https://www.hlb.de/fileadmin/hlb-global/downloads/Positionen/2025-10-13_hlb-Positionspapier_HoeD.pdf

Honekamp, W., & Klingelhöfer, K. (Hrsg.). (2025). Polizei-Informatik 2025. Deutsche Hochschule der Polizei. https://dhpol.de/Bd_27pdfA.pdf

Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., & Labudde, D. (2023). Technologiegetriebene Polizeiausbildung im Umgang mit digitalen Spuren. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie 2: Phänomene und Auswirkungen* (S. 673–702). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-35442-8_51

INTERPOL Innovation Centre. (2026). Innovation Snapshots 6(2). https://www.interpol.int/en/content/download/24374/file/Innovation%20Snapshots%20April%202026.pdf

Koper, C. S., Lum, C., & Willis, J. J. (2014). Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and behavioural aspects of implementing police technologies. *Policing*, *8*(2), 212–221. https://doi.org/10.1093/police/pau015

Koper, C. S., Taylor, B. G., & Woods, D. J. (2015). *Realizing the potential of technology in policing: A multisite study of the social, organizational, and behavioral aspects of implementing police technologies*. Police Executive Research Forum / National Institute of Justice.

Kriegesmann, B., Kerka, F., & Kottmann, M. (2007). Innovationen werden von Menschen gemacht: Kompetenzentwicklung jenseits von Weiterbildung und Wissensmanagement. In B. Kriegesmann & F. Kerka (Hrsg.), Innovationskulturen für den Aufbruch zu Neuem (S. 177–208). DUV. https://doi.org/10.1007/978-3-8350-9488-8_5

Lum, C., & Koper, C. S. (2015). *The need for more research on police technology*. Testimony for the President's Task Force on 21st Century Policing. Center for Evidence-Based Crime Policy. George Mason University. https://ascpolicing.org/wp-content/uploads/2015/03/LumKoperTechnology.pdf

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly*, *20*(2), 135–163. https://doi.org/10.1177/1098611116667279

Ordon, G., Dewar, L., & Cameron, A. (2019). Leadership, wellbeing, professional development and innovation for the police front line: An evidence review. College of Policing. https://assets.publishing.service.gov.uk/media/5d25bb79ed915d69031d7c8b/FLR_literature_research_report.pdf

Police Foundation/PERIL. (2024). *Emerging police technology: A policy toolkit*. Criminal Justice Policy Program. Harvard Law School, Stanford Criminal Justice Center. Stanford Law School. https://law.stanford.edu/wp-content/uploads/2020/01/Emerging-Police-Technology-A-Policy-Toolkit.pdf

Police Science and Technology Advisory Council / UK Home Office. (2024). *Police emerging science and technology trends (PESTT): Annual report 2024*. Office of the Police Chief Scientific Adviser. https://science.police.uk/site/assets/files/5939/pestt_report.pdf

Rektorenkonferenz der Hochschulen für den öffentlichen Dienst. (2023). Angewandte Forschung an den HöD / Forschungsförderung. Positionspapier/Resolution. https://www.hs-kehl.de/wp-content/uploads/Resolution_Angewandte-Forschung-HoeD_06.2023.pdf

Ruch, A., Salzmann, V., & Wickert, C. (2025). Rechenschaftsbericht zum Studienjahr 2024/25. Institut für Polizei- und Kriminalwissenschaften, HSPV NRW. https://www.hspv.nrw.de/dateien_forschung/forschungsinstitute/ipk/IPK_Rechenschaftsbericht_2024-25.pdf

Sächsisches Institut für Polizei- und Sicherheitsforschung. (2024). Jahresbericht 2023. Hochschule der Sächsischen Polizei (FH). https://www.polizei.sachsen.de/de/download/PolFH/SIPS_Jahresbericht_2024_05_09_2025.pdf

Sun, C. M., Coldren, J. R., Jr., & Blondin, A. P. (2025). The smart policing initiative: 15 years of evidence-based innovation in policing practice. Justice Evaluation Journal, 8(2), 129–149. https://doi.org/10.1080/24751979.2025.2474121

Die Bedeutung von Technischen Richtlinien für Einsatzhelme in Zeiten zunehmender innerstaatlicher Gewalt

Lothar H. Schuster

Heutzutage stehen der Bereitschaftspolizei (BePo) und den polizeilichen Spezialeinsatzkommandos (SEK) des Bundes und der Länder jeweils spezifische Kopfschutzsysteme auf internationalem Spitzenniveau zur Verfügung. Beide Helmtypen dienen dem bestmöglichen Schutz vor unterschiedlichen Bedrohungen: Der Einsatzhelm für Bereitschaftspolizeien bietet Schlag- und Stichschutz und der Einsatzhelm für Spezialeinsatzkommandos ballistischen Schutz.

Der Weg zu dieser Technologieführerschaft soll im Nachfolgenden zum ersten Mal näher betrachtet werden. Der Autor hat die Entwicklungen im beginnenden 21. Jahrhundert in verschiedenen Verwendungen in der Zulieferindustrie aktiv begleitet und nun erstmalig mit wesentlichen Dokumenten zusammengefasst.

Bereits zu Beginn des 21. Jahrhunderts waren deutsche Polizeien im Bereich des berufsspezifischen Kopfschutzes recht gut aufgestellt, denn Lehren aus dem Einsatz hatten für eine stetige Weiterentwicklung der beschafften Helme gesorgt.

Einer der Gründe dafür war, dass die Vorgängerorganisation des Polizeitechnischen Institutes (PTI) der Deutschen Hochschule der Polizei (DHPol), die am 17.02.1975 an der Polizei-Führungsakademie (PFA) gegründete Forschungs- und Entwicklungsstelle für Polizeitechnik (FEStPt), über viele Jahre nicht nur die technische Entwicklung für die föderalen Polizeistrukturen zentral koordinierte, sondern auch den Fachinformationsaustausch auf internationaler Ebene sicherstellte. Im Oktober 1997 war dann das PTI als Nachfolgeorganisation der FEStPt etabliert worden. Das PTI trat der im Herbst 1999 auf Initiative von Dr. Dr. Beat Kneubuehl[1] gegründeten Vereinigung der Prüfstellen für angriffshemmende Materialien und Konstruktionen (VPAM) bei und war bis zum Austritt am 13.10.2022 nicht nur Mitglied, sondern auch Geschäftsstelle der VPAM − einem Zusammenschluss amtlicher (ziviler und militärischer) Prüfstellen von mehreren europäischen Staaten, die durchschusshemmende, stich- und schlaghemmende Schutzausrüstungen nach bestehenden nationalen und internationalen Standards prüfen, mit dem Zweck, den Erfahrungsaustausch, die gegenseitige Unterstützung in technischen Belangen (so z. B. bei der Standardisierung und teilweise auch zur gemeinsamen Beschaffung von Prüfmitteln) und die gegenseitige Information zu fördern.

Der Schutzhelm für Bereitschaftspolizeiaufgaben

Am Anfang stand der Beschluss der Ständigen Konferenz der Innenminister vom 08.02.1968 vor dem Hintergrund einer stetig zunehmenden Zahl unfriedlich verlaufender Demonstrationen: „Die Polizeibeamten sind für Einsätze bei Demonstrationen und dgl., die einen unfried-

[1] Dr. sc. forens. Dr. med. h. c. Dipl.-Math. Beat Paul Kneubuehl ist ein Schweizer Mathematiker und Ballistiker. Er arbeitete von 1974 bis 2006 als wissenschaftlicher Mitarbeiter im Fachgebiet Ballistik in der Abteilung für Ballistik/Schiessversuche der Gruppe für Rüstungsdienste (heute: armasuisse, Wissenschaft und Technologie) des VBS.

lichen Charakter annehmen können, mit einem Kunststoffhelm mit Augenschirm, Ohren- und Nackenschutz auszustatten. Der Kunststoffhelm soll einheitlich in den Ländern in weißer Farbe ausgeführt sein. Die Beschriftung bleibt den Ländern überlassen“ (Kienle, 1968, S. 457).

Zur besseren Nachvollziehbarkeit der Helmentwicklung hat der Autor die Helmentwicklung von 1968 bis heute in Generationen klassifiziert:

- **Generation 1**:
  Spritzgusskalotte in Halbschalenform in Anlehnung an die Form des Innenhelms des amerikanischen M1-Stahlhelms (eingeführt ab 1968).
- **Generation 2**[2]:
  Spritzgusskalotte in Jethelm-Form mit Höröffnungen (eingeführt ab 1969).
- **Generation 3**:
  Aramidkalotte in Jethelm-Form ohne Öffnungen nach TR 1992 (eingeführt ab 1992).
- **Generation 4**:
  Aramidkalotte in Jethelm-Form ohne Öffnungen nach TR 1992 mit zusätzlicher Flammschutzoptimierung (eingeführt ab 2001).
- **Generation 5**:
  Aramidkalotte in Jethelm-Form ohne Öffnungen nach TR 2011 (eingeführt ab 2015).

Im August 1992 hatte die Technische Kommission des AK II erstmals mit der Technischen Richtlinie (TR) für ein modular aufgebautes System - Schutzhelm, Hör-/Sprechgarnitur, Atemschutzmaske - (TR 1992) die wesentlichen Einsatzerfahrungen seit dem Ersteinsatz derartiger Helme während der Studentenunruhen 1968 in ein neuartiges Anforderungsprofil umgewandelt, das sich in den Folgejahren bewähren sollte. Diese Richtlinie verlangte nicht mehr nur Schlagschutz, sondern auch adäquaten Stichschutz aller Komponenten (Kalotte, Visier und Nackenschutz) sowie die Möglichkeit des Einsatzes als Helm-Masken-Kombination. Denn am 25.11.1978 hatte ein Polizist in Frankfurt eine schwere Kopfverletzung erlitten, als ihn ein iranischer Demonstrant mit einer von einer Baustelle mitgenommenen Baukrempe am Helm traf. Die Baukrempe durchschlug die Spritzguss-Kalotte und das innenliegende EPS-Stoßdämpfungselement (Radecke, 1981, S. 162).

Die Helm-Masken-Kombination wurde zunächst für den Bereich der Feuerwehr entwickelt. Die Firma Dräger hatte ab 1975 begonnen, eine neuartige Maskenanbindung für den Feuerwehrhelm zu entwickeln (Herminghaus, 1982, S. 102−103). Im Auftrag des Bundesministeriums für Forschung und Technologie hatte die Firma Porsche AG von 1976 bis 1978 die O.R.B.I.T.[3]-Studie durchgeführt; in dieser Studie wurde auch eine Helm-Masken-Kombination für die Feuerwehr designt (Herminghaus, 1982, S. 104−105). Dieses Konzept wurde für die Polizei übernommen, damit Einsatzkräfte beim Einsatz von Tränengas den Helm nicht mehr ablegen mussten, um die Atemschutzmaske anzulegen, wenn sie sich in Reichweite der Demonstranten befanden. Denn nach Einführung von Wasserwerfern hatten Demonstranten begonnen, die Strahlrohrkuppeln mit selbst gebauten Zwillen und Metallkugeln aus Kugellagern zu bekämpfen („Harter Aufschlag! Große Genauigkeit!“, 1986, S. 28). Weder das

[2] Die Polizeien der DDR hatten zum Zeitpunkt der Wiedervereinigung Helme technisch vergleichbar mit der Generation 2 in der BRD.
[3] Optimierte Rettung Brandbekämpfung mit integrierter technischer Hilfeleistung.

Verbot von Präzisionszwillen mit Armstützen im Waffengesetz 1978 noch die Beimischung von Tränengas beim Wasserwerfer schafften zunächst ausreichend Abhilfe. Aufgrund der Durchschlagsleistung der Stahlkugeln mussten die Wasserwerfer von Einsatzkräften begleitet werden, um für besseren Schutz der Spezialfahrzeuge im Nahbereich zu sorgen. Dabei erlitten Einsatzkräfte häufig erhebliche Kopfverletzungen durch Stahlkugeln oder bis zu tennisballgroße Steine, wenn sie beim Einsatz von Tränengas kurzzeitig ihren Helm ablegen mussten, um die Atemschutzmaske anzulegen. Denn Tränengas wurde damals nicht nur von der Polizei, sondern auch vom polizeilichen Gegenüber eingesetzt (Zahn, 1986, S. 3).

Insbesondere im Bereich Schlag- und Stichschutz hatte die FEStPt umfangreiche Vorarbeit geleistet; ab 1980 hatte man an einer Prüfvorschrift für Einsatzhelme gearbeitet und nach intensiven Tests 1982 unter anderem mit einem Schlagstock aus Kunststoff, einer genagelten Holzlatte, einem Pflasterstab und einer Bauklammer (Forschungs- und Entwicklungsstelle für Polizeitechnik, 1982, S. 1) entschieden, dass die Stoßdämpfungsanforderungen der DIN 4840 für Arbeitsschutzhelme nicht mehr ausreichend und zukünftig die Stoßdämpfungsprüfverfahren der europäischen Motorradhelmnorm ECE 22.03 zur Prüfung von Einsatzhelmen anzuwenden sind.

Mit der Einführung der ersten Helme nach TR 1992 wurden die aus gespritztem Kunststoff bestehenden Helme des vormaligen Marktführers Römer Helme aus Neu-Ulm[4] sukzessive aus der Nutzung genommen[5], da dieser Kunststoff bei der Prüfung mit dem definierten Dorn keinen normkonformen Stichschutz mehr bieten konnte. Die neue Helm-Masken-Kombination deckte mit einer Helmkalotten- und einer Schutzmaskengröße den Kopfgrößenbereich von 53 bis 62 ab und hatte die Option für eine helmabhängige[6] Hör-/Sprechgarnitur. Dazu war im Nackenpolster eine Einschubmöglichkeit für den Ohrhörer vorgesehen und im Oberkopfbereich konnte in die geschäumte Polystyrolschale ein bereits im Feuerwehrbereich bewährtes Schädeldeckenmikrofon eingebracht werden (Auergesellschaft GmbH & Schuberth Helme GmbH, 1995, S. 2–3).

2002 übernahm dann die US-Firma MSA den französischen Helmhersteller CGF Gallet (Ferrand & Zaglia, 2005, S. 157) und entwickelte intern ein eigenes Helmsystem; eines von bisher nur zwei Systemen[7], bei dem Helm (MO 5006) und Schutzmaske (Schutzmaskentyp Auer 3S-H) vom selben Hersteller kommen. Der bisherige Helmpartner, die Schuberth Helme GmbH, arbeitete dann mit dem Schutzmaskenhersteller Dräger Safety AG & Co-KGaA (Schutzmaskentyp Panorama Nova) weiter. Beide Helmtypen hatten ein unterschiedliches Doppelgrößensystem. Dies führte im Rahmen einer Großbeschaffung des Bundes für einige Jahre zu Komplikationen. Denn der Bund hatte zunächst für die Bereitstellung von Einsatzhelmen

[4] Die Firma Römer Helme wurde 1995 vom US-Helmhersteller Bullard übernommen; 2005 wurde die Produktion der Römer Polizeihelme gänzlich eingestellt; technisch vergleichbare Helmtypen werden aber bis heute produziert.

[5] Nach der Wiedervereinigung hatten die Polizeien der alten Bundesländer zumeist bereits begonnen, Helme nach TR 1992 zu beschaffen und ihre alten Römer Helme in Amtshilfe an die Beitrittsländer abzugeben, um deren ebenfalls aus gespritztem Kunststoff bestehenden Einsatzhelme aus DDR-Fertigung zu ersetzen.

[6] Mittlerweile wird helmunabhängigen Hör-/Sprechgarnituren der Vorzug gegeben, da sie im Einsatz auch getragen werden können, wenn der Helm nicht getragen werden muss (Schuberth GmbH, 2015, S. 4).

[7] Vorher gab es von Dräger ein System bestehend aus dem Helmtyp Diamant (produziert von CGF Gallet) und der Dräger-Maske Panorama Nova.

für die Polizeien der Länder Größenverpasssätze des einen Herstellers beschafft und später aber nach der Ausschreibung Helme des anderen Herstellers geliefert, sodass die gelieferten Helme wegen Größenproblemen häufig abgelehnt wurden und die Länderpolizeien in Eigenverantwortung den jeweils bevorzugten Einsatzhelmtyp anschafften.

Im Bereich von Waffen und Munition für die Polizei ist es bewährte Praxis, nach erfolgreichem Durchlaufen aller Prüfungen gemäß einer Technischen Richtlinie die Prüfzeugnisse durch eine akkreditierte Zertifizierungsstelle überprüfen und ein Zertifikat ausstellen zu lassen. Die einzige deutsche VPAM-Prüfstelle, die gleichzeitig auch als Zertifizierungsstelle akkreditiert ist, ist das Beschussamt in Ulm. Körperschutz wird aber traditionell im Beschussamt Mellrichstadt geprüft. Somit ergab sich die Problematik der Zertifizierung dieser Art von Einsatzhelmen. Zum ersten und einzigen Mal hatte zunächst das PTI am 27.07.2004 richtungsweisend der Firma MSA Auer GmbH das Zertifikat Nr. SH-AM 01 04 für die Anteile Schutzhelm und Atemschutzmaske ausgestellt. Denn zu dieser Zeit galt die Regel, dass bei der Helm-Masken-Kombination der Helm nur eine andere Art der Maskenbefestigung darstellt und daher der Schutzmaskenhersteller die Prüfung und Zertifizierung anmelden musste. Man wies aber seitens des PTI damals bereits darauf hin, dass diese Zertifizierung ein Einzelfall bleiben werde.

Der Einsatzhelm für Spezialeinsatzkommandos

Erst nach dem Attentat während der Olympischen Spiele 1972 waren in Westdeutschland polizeiliche Spezialeinheiten aufgestellt worden, die zunächst mit einem handelsüblichen Stahlhelm ausgestattet wurden. Ab 1976 begann dann die Entwicklung und Einführung von ballistischen Schutzhelmen aus Titan. Einsatzerfahrungen führten um 1990, maßgeblich beeinflusst durch den damaligen Kommandeur der Grenzschutzgruppe 9 (GSG 9), zur Einwicklung einer neuen Helmgeneration aus Titan mit angeschweißten Seitenteilen (für das Tragen von Kapselgehörschutz); einen kleineren Marktanteil hatte zeitweise auch ein Helmmodell aus Aramid. Mit Unterstützung der Koordinierungsstelle der Spezialeinheiten Nordrhein-Westfalen entstand dann 2005 ein patentierter Titanhelm mit nahtlos gezogenem Ohrbereich.

Die FEStP hatte dazu bereits im Dezember 1982 die heute weitgehend unbekannte Richtlinie Anforderungen und Prüfvorschrift für „beschusshemmenden“ Kopfschutz herausgebracht. Interessanterweise sah diese Vorschrift bereits 4 Schutzklassen vor (I+II: Kurzwaffe/Maschinenpistole, III: Langwaffe, IV: Langwaffe mit Hartkerngeschossen). Geprüft wurde allerdings nur die Halteleistung der Kalotte; die dynamische Verformung der Kalotte beim Beschuss wurde noch nicht geprüft.

Nachdem erste Einsatzerfahrungen vorlagen, legte auch hier der Unterausschuss Führungs- und Einsatzmittel (UA FEM) des Arbeitskreises II „Innere Sicherheit“ der Arbeitsgemeinschaft der Innenministerien der Länder im Januar 1997 die Technische Richtlinie (TR) Durchschusshemmender Helm (TR 1997) auf. Bei dieser Art von Helmen kommt es nun nicht mehr nur auf das Stoppen des Geschosses an, sondern auch darauf, dass keine oder nur möglichst geringe Restenergie durch die dynamische Verformung des Helmes beim Beschuss auf den Schädel übertragen wird, um Kopfverletzungen so weit wie möglich zu verhindern. Um dies zu überprüfen, hieß es in der TR vom Januar 1997 auf Seite 11 unter 3.5.3: „Zur Ermittlung

der dynamischen Ausbeulung wird, falls bei Treffer Nr. 1 und Nr. 28 kein Durchschuss erzielt wurde, vor dem 3. Schuss auf der Innenseite der Helmschale ein Ausbeulungsmesskopf im Abstand von 10 mm zur Helmschale angeordnet. Die Bestimmung der dynamischen Ausbeulung erfolgt nach dem Beschuss durch Messung der Deformation des Messkopfes zuzüglich 10 mm Distanz. Die dynamische Ausbeulung darf den Abstand zwischen Helmschale und Kopf nicht überschreiten." Bei der Anwendung dieser TR stellte man im Laufe der Zeit fest, dass dieses Verfahren zur Ermittlung der dynamischen Ausbeulung zu wenig aussagekräftig und zu anfällig war. Denn vor dem Prüfbeschuss wurden die Innenausstattung und der Kinnriemen entfernt und nur die eingespannte Kalotte punktuell beschossen, sodass am Ende einer Prüfung ein Ergebnis stand, das im Wesentlichen auf der Herstellerzusicherung des definierten Abstandes zwischen der Innenausstattung und der Kalotteninnenseite beruhte.

Neue Bedrohungen

Nach dem Ende des Kalten Krieges und der deutschen Wiedervereinigung geriet das Thema Sicherheit gesamtgesellschaftlich zunehmend in den Hintergrund. Durch den Ukrainekrieg wissen wir heute im Bereich der äußeren Sicherheit, welche Konsequenzen dies nach sich zog. Aber auch im Bereich der inneren Sicherheit zeichnete sich eine ähnliche Entwicklung ab, obwohl die Gewalt im Inneren kontinuierlich, von der Öffentlichkeit häufig unbeachtet, zunahm. Dies führte dazu, dass die Bedeutung des Polizeitechnischen Institutes für die Erhaltung/Dokumentation des notwendigen Fachwissens – auch dies zunächst polizeiintern weitgehend unbemerkt – immer weiter anstieg (Schröder, 2005a, S. 28).

Am 23.03.1994 hatte sich auf der Autobahn 5 bei Langen/Mörfelden ein kurdischer Demonstrant selbst in Brand gesetzt und brennend versucht, Polizeibeamte anzugreifen; zusätzlich wurden auch Brandbeschleuniger gegen die Polizei eingesetzt (Schröder, 2005b, S. 109). Einer der Einsatzleiter von der BFE 590 (Frankfurt) der hessischen Polizei, der spätere EPHK Wilhelm Schröder, führte im Nachgang eine Gefährdungsanalyse der damaligen persönlichen Ausrüstung der Einsatzkräfte mit verheerendem Ergebnis durch. In unzähligen Brandversuchen wurden die Schwächen aller Ausrüstungsteile (Helm, Einsatzanzug, Handschuhe, Stiefel etc.) untersucht und ein neues Bekleidungskonzept erarbeitet.

Als besonders gefährlicher Schwachpunkt wurde dabei ein Flammunterschlag auf der Frontseite bis unter den Helm identifiziert, da dort bisher aus Gründen der Mobilität und der Belüftung wesentliche Partien von Hals, Kinn und Gesicht ungeschützt waren.

Daher wurde auch ein neues Prüfverfahren für Helme mit besonderem Einsatzbezug erarbeitet: Dieser weltweit einzigartige Brandtest für Helm, Schutzmaske, Hör-/Sprechgarnitur und ggf. Kinn-/Mundschutz (Kinnbügel) simuliert einen Brusttreffer mit einem Molotow-Cocktail und einen dadurch verursachten Flammunterschlag.

[8] 9 x 19mm mit 8 g. Vollmantelrundkopf-Geschoss mit einer V_3 von 410 ± 10 m/s.

Abb. 1: Einsatzhelm der Generation 2 nach Brandtest

Abb. 2: EPHK Schröder beim Test verbesserter Materialien

Dieser Test löste nach Einführung immer wieder Diskussionen aus, denn Hersteller mussten des Öfteren feststellen, dass ihre Systemkomponenten, die bereits für die Feuerwehr zugelassen waren, diesem Test nicht standhielten. Da jeder Test einen individuellen Beflammungsverlauf hat, wurde gelegentlich die begrenzte Vergleichbarkeit und Reproduzierbarkeit dieses Prüfverfahrens bemängelt. Dies war aber genauso bei der Einführung beabsichtigt, da bei diesem Testverfahren ein Hersteller gezwungen ist, sein Produkt auf das Worst-Case-Szenario hin zu entwickeln, und Produktoptimierungen für ein berechenbares Prüfszenario vermieden werden.

Abb. 3: Brandprüfung gemäß TR 2011

Polizeiintern zeigte dieser Test auf, dass zukünftig das Tragen einer flammhemmenden Kopfschutzhaube aus Arbeitsschutzgründen nicht mehr verwehrt werden kann. Bis dato wollten nämlich die Einsatztaktiker aus rechtlichen Gründen eine „Vermummung" der Einsatzkräfte vermeiden[9]. Da aber Brandwunden am Hals sehr schwere Einschränkungen für die Motorik des Kopfes haben können, wurde als Kompromiss die flammhemmende Kopfschutzhaube mit offenem Gesicht (und nicht die Variante der Spezialeinheiten mit Augenschlitz) eingeführt. Somit wurde nicht nur die Vermummung verhindert, sondern auch die Kompatibilität mit der Atemschutzmaske (wie bei der Feuerwehr) gewahrt.

Aus eigenem Antrieb teilte EPHK Schröder seine Ergebnisse aus unzähligen eigenen Versuchen intensiv mit anderen Polizeien, dem PTI und auch interessierten Herstellern. Der Autor lernte ihn im September 1999 mehr oder weniger zufällig bei einem Seminar der Fachzeitschrift POLIZEI-heute des EPHK a. D. Helmut Brückmann in Braunschweig kennen. Als Sohn eines NRW-Polizeischulrektors und Reserveoffizier der Bundeswehr war der Autor von den umfassenden Erkenntnissen bzgl. der Gefährdung durch Feuer im Einsatz sehr überrascht,

[9] Die Identifizierbarkeit der einzelnen Einsatzkraft muss weiterhin gewährleistet bleiben. Dies wird heutzutage zumeist durch sichtbare Nummernsysteme auf der Ausrüstung ermöglicht.

sodass sich ein intensiver Austausch anschloss. Als erste Problematik wurde die bis dato weitgehend erfolglose Bekämpfung des Visierbeschlagens im Einsatz angegangen. Mit der gemeinsamen Prüfung und erfolgreichen Einführung der aus dem Motorradhelmbereich stammenden Doppelscheibentechnologie (Markenname Pinlock®) wurde erstmals eine funktionale Problemlösung eingeführt[10]. Zusammen entstand dann auch der erste in Bezug auf Flammhemmung besonders optimierte Einsatzhelm (P100F). Von wesentlicher Bedeutung bei dieser Entwicklung war auch das Fachwissen von Uwe Barth, damals Entwicklungsleiter der Firma Schuberth Helme GmbH:

Mittwoch, 29. Mai 1968 — BRAUNSCHWEIGER ZEITUNG — Seite 23

Polizisten sollen ruhig mal ihren Kopf hinhalten können

Braunschweiger Werk entwickelte „schlagsicheren" Helm

Die Polizei in den Bundesländern soll so schnell wie möglich mit modernen Schutzhelmen ausgerüstet werden, weil Polizisten bei Demonstrationen in der Karwoche und später in mehreren Städten Kopfverletzungen davongetragen haben. Unter den Firmen, die gebeten worden sind, einen geeigneten Helm zu entwickeln, ist auch ein Braunschweiger Unternehmen.

Erste Prüfungen haben bereits stattgefunden, so in Berlin, wo 6000 Polizisten einen Schutzhelm bekommen sollen. Gesucht wird ein Helm, unter dem Polizisten ruhig einmal „ihren Kopf hinhalten" können. Die Entscheidung über das beste Modell oder auch über die vorteilhafteste Kombination mehrerer Entwürfe dürfte nach einer an diesem Mittwoch im Polizeiinstitut Hiltrup stattfindenden Generalvorführung fallen.

● An der Spitze der bisherigen Beurteilungen liegt das Modell der Schuberth-Werke in Braunschweig, deren Spezialität (für den Export in 70 Länder) Schutzbekleidung aller Art ist. Dieses Modell wurde von Konstrukteur Wilfried Berge entworfen, der mit mehr als hundert Typen brauchbarer Schutzhelme, die er schon geschaffen hat, auf eine reiche Erfahrung zurückgreifen konnte.

„Der kräftigste Mann wird versagen, wenn er — ganz gleich, ob mit einem Gummi- oder Holzknüppel oder sogar mit einer Eisenstange — auf diesen neuen Helm für die Polizei einschlägt", verspricht Wilfried Berge. „Dem Träger entsteht kein ernster Schaden, er zieht sich weder einen Genick- noch einen Schädelbruch zu."

Er hat sein Modell härtesten Prüfungen unterworfen. Die Sicherheit des Trägers wird noch durch einen besonderen Gesichts- und Nackenschutz erhöht. Alle Teile sind aus thermoplastischem Kunststoff, wie er für beschußsichere Westen verwendet wird. So ist der Gesichtsschutz splitterfest; ein Luftgewehr zum Beispiel hinterläßt nicht die geringste Spur.

● Der Nackenschutz wird durch Spezialnylon gewährleistet. Er wurde unter anderem durch Schläge mit einem Holzknüppel erprobt, in den Nägel eingelassen waren: sie vermochten den Nackenschutz nicht zu durchdringen.

Ein Gabel-Kinnriemen (nach dem Vorbild der Fallschirmspringerhelme garantiert, daß der Schutzhelm, der auf alle Kopfgrößen einstellbar ist, völlig fest sitzt. Neben Schweißleder und Gurtbändern hat er eine Hartschaum-Auskleidung, um besondere Härte der Schläge zu dämpfen.

Neben allen Überlegungen, dem Träger optimale Sicherheit zu geben, war auch die Aufgabe gestellt worden, einen in seiner Form „schicken" Helm zu entwerfen, der den Polizisten nicht etwa dem Gespött der Demonstranten aussetzt. Aus diesem Grunde wurde von vornherein auf eine „raumfahrerähnliche" Konstruktion verzichtet.

hei-

SCHLAGSICHER UND SCHICK: Der von einem Braunschweiger Werk entwickelte Polizeischutzhelm. Foto: Wesemann

Schwurgericht verhandelt wegen Mordes

Sitzung beginnt Mitte Juni — Auch der Braunschweiger „Fall Sestrup" steht an

Mitte Juni beginnt im Landgericht Braunschweig die zweite Sitzungsperiode des Schwurgerichts in diesem Jahr. Drei Termine stehen im Kalender des Vorsitzenden, Landgerichtsdirektor Dr. Rüdiger Hauswaldt: Der Mordprozeß gegen Bernhard Sestrup, der angeklagt ist, in Braunschweig zwei Menschen getötet zu haben, die Verhandlung gegen Isolde Blum, die ihren Geliebten in Braunlage mit einem Beil erschlug, und ein Prozeß gegen eine Mutter wegen Kindestötung.

Laufe der Verhandlung sollen 18 Zeugen und ein Sachverständiger gehört werden. Auch plant das Schwurgericht, sich durch eine Besichtigung des Tatortes in Salzdahlum über die örtlichen Verhältnisse zu unterrichten.

Sestrup, der die ihm zum Vorwurf gemachten Taten bisher nicht geleugnet hat, wird von dem Sachverständigen als voll verantwortlich im Sinne des Gesetzes bezeichnet. Der Intelligenzgrad des Angeklagten liege jedoch zwischen Schwachsinn und Be-

einen Faustschlag versetzt habe, berichtete die Angeklagte bei ihrer Vernehmung.

Das will sie dann auch getan haben. Da Starke nach dem ersten Schlag, der ihn unvorbereitet traf, zu Boden stürzte und röchelte, hielt ihm die Angeklagte den Mund zu und schlug noch ungefähr zwanzig Mal auf den Kopf ihres Geliebten ein.

In den folgenden Tagen besuchte Isolde Blum tagsüber Gaststätten, schlief aber nachts neben der Leiche

Abb. 4: U. Barth mit dem P68 in der Braunschweiger Zeitung

Die Entwicklung des ersten Polizeieinsatzhelmes dieser Firma war 1968 sein Erstlingswerk gewesen und er hatte danach maßgeblich nicht nur die Helmentwicklung für Arbeitsschutz, Feuerwehr, Militär, Motorrad, Polizei, Zivilschutz, sondern auch die dazugehörige Normenarbeit entscheidend zunächst im deutschsprachigen, später sogar im europäischen Raum geprägt. Ohne diese einzigartige Expertise wäre eine zeitnahe Umsetzung des neuen Forderungskataloges nicht realisierbar gewesen.

Während sich das verbesserte Helmmodell der Generation 4 zunehmend bei den Polizeien durchsetzte, blieb die begleitende Normenarbeit allerdings zunächst erfolglos; 2006 und 2008 vom PTI vorgelegte Richtlinienentwürfe wurden nicht in Kraft gesetzt. Somit waren die Bundesländer bei Ausschreibungen zunächst gezwungen, sich bei der Hessischen Polizei deren Technische Lieferbedingungen (TL) Einsatzhelm Hessen-Stand 11.2000 zu beschaffen und zusammen mit der TR 1992 in ihren Ausschreibungen zu verwenden.

[10] Heutzutage werden alternativ auch auf der Innenseite antibeschlagbeschichtete Visiere eingesetzt.

Die Technischen Richtlinien für Schutzhelme von 2010 und 2011

Bei einer Richtliniendiskussion des Autors mit den damaligen zuständigen Akteuren des PTI, dem Leiter, Leitender Regierungsbaudirektor Dipl.-Phys. Hans-Rudolf Damm, und dem zuständigen Technischen Angestellten Dipl.-Ing. Günther Langer, die beide in absehbarer Zeit vor der Pensionierung standen, zeichneten sich bereits massive Schwierigkeiten für die Fortschreibung der TR aufgrund der seinerzeit unsicheren Zukunft des PTI ab (Hans, 2017, S. 34–35).

Abb. 5: H.-R. Damm (links) und G. Langer (rechts)

Der Autor bot daraufhin an, quasi als persönliches Abschiedsgeschenk, aber insbesondere auch als länger bleibende Erinnerung mit Mehrwert für die Polizeien des Bundes und der Länder, das auf-den-Weg-bringen zweier neuer TR zu unterstützen.

Die Fortschreibung der TR 1997

Der Leitende Regierungsbaudirektor Damm betrachtete als größtes Hindernis, dass für die Fortschreibung der TR 1997 zunächst ein Workshop mit allen Spezialeinheiten des Bundes und der Länder notwendig sei, um die Erstellung eines neuen Anforderungsprofils für einen durchschusshemmenden Helm zu ermöglichen, auf dessen Grundlage eine neue Technische Richtlinie Durchschusshemmender Helm erstellt werden könnte. Allerdings hatte es bis dahin eine derartige Veranstaltung am PTI noch nicht gegeben. Der Autor nahm dies als Herausforderung an und konnte nach einiger Zeit dem PTI melden, dass alle deutschen Spezialeinheiten anwesend sein würden. Dadurch konnte dann vom 01.07. bis 02.07.2009 an der DHPol ein für alle Beteiligten denkwürdiger Workshop stattfinden. Folgende Firmen tru-

gen ihre Überlegungen vor (Deutsche Hochschule der Polizei, 2009, S. 1): Busch GmbH & Co. KG (Egon Busch), Dräger Safety AG & Co-KGaA (Daniel Budde), DSM Dyneema (William Roovers), Ulbrichts Witwe GmbH (Franz Rieger) und Schuberth GmbH (Lothar Schuster). Zur Darstellung bisheriger Einsatzerfahrungen und daraus abgeleiteter Wünsche/Forderungen der Spezialeinheiten an einen durchschusshemmenden Helm konnte der in Ost- und West-Spezialeinheiten erfahrene PHK Roger Klose vom SEK Sachsen-Anhalt (Magdeburg) gewonnen werden. Im Nachgang zu diesem Workshop entstand dann die bis heutige gültige TR 2010. Dr. Dr. Beat Kneubuehl hatte parallel ein neues Verfahren zur Messung der dynamischen Verformung der Kalotte entwickelt und in einer VPAM-Spezifikation (PRÜFRICHTLINIE VPAM HVN 2009 „Durchschusshemmender Helm mit Visier und Nackenschutz“) festgeschrieben, die in die TR 2010 als Prüfvorschrift Einzug hielt. Zur Ermittlung der dynamischen Verformung wird dabei der vollständige Helm (mit Innenausstattung und Kinnriemen) auf einem Prüfkopf aus ballistischer Seife der Größe 62 (Kopfform gemäß ECE 22.03) befestigt und bei Raumtemperatur beschossen. Danach wird in einem spezifizierten Verfahren die übertragene Restenergie ermittelt. Diese darf nicht größer als 25 Joule sein. Dieser Wert wurde aus dem Boxsport übernommen. Er wird dort als Grenzwert betrachtet, ab dem irreversible Schädigungen des Gehirnes auftreten können.

Nach der zügigen Zustimmung des Bundes und der Länder zu dieser TR wurde eine neue Titanhelmgeneration entwickelt, die ab 2011 Einzug in die Spezialeinheiten hielt.

Ein neues Helmmodell nach TR 2010

Nach den Amokläufen mit Schusswaffeneinsatz (Erfurt 2002, Winnenden 2009) und dem einsetzenden arabischen Terror entschieden sich die Polizeien, sukzessive das sogenannte First-Responder-Konzept einzuführen. Dieses Konzept sieht vor, dass die als Erstes am Einsatzort eintreffenden Polizeikräfte nicht mehr nur absichern und auf das SEK warten, sondern direkt aktiv in die Lage eingreifen und versuchen, die Lage einzugrenzen oder sogar zu beenden, um möglichst viele Menschenleben zu erhalten. Dazu musste die Ausstattung der Streifenwagen ergänzt werden: zwei Plattenträger (um die weichballistische Standardschutzweste im Schutzniveau VPAM 3 auf Langwaffenschutz VPAM 6 zu erhöhen), zwei ballistische Schutzhelme mit Kopfgrößenschnellverstellung sowie eine Mitteldistanzwaffe (Maschinenpistole oder Sturmgewehr). Für die Ausschreibung und Beschaffung dieses neuen **First-Responder-Helmtyps** wurde die TR 2010 auch von der überwiegenden Zahl der Polizeien genutzt.

Mittlerweile haben die Firmen Ulbrichts GmbH (vormals Ulbrichts Witwe GmbH) und Busch PROtective Germany GmbH & Co. KG die Prüfverfahren dieser TR durch Entwicklungen für diesen neuen Bedarf nahezu weltweit bekannt gemacht; der Firma Busch PROtective ist es 2019 sogar gelungen, amerikanische Behörden wie die Drug Enforcement Administration (DEA), das Federal Bureau of Investigation (FBI), den United States Marshals Service (USMS) und das Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) von nach dieser Prüfmethodik entwickelten Helmen zu überzeugen (Busch PROtective Germany GmbH & Co. KG, o. D.).

Diese TR 2010 hat sich demnach nicht nur als verlässlicher Sicherheitsfaktor für deutsche Einsatzkräfte, sondern auch als Innovationsmotor mit weltweiter Strahlkraft bewährt. Und die Entwicklung steht nicht still, der bisherige Schutz gegen Kurzwaffenmunition wird aktuell durch neue, bereits marktverfügbare Produkte übertroffen, die sogar Schutz gegen Langwaffenmunition bieten.

Die Fortschreibung der TR 1992

Nach der Pensionierung von H.-R. Damm am 30.09.2010 schaffte es Günther Langer nahezu im Alleingang, die Technische Richtlinie von 1992 auf Basis der Entwürfe von 2006 und 2008 fortzuschreiben und durch föderale Zustimmung noch vor seinem Ausscheiden in Kraft zu setzen. Im Februar 2011 gab das PTI die modifizierte „Technische Richtlinie für ein modular aufgebautes System „Schutzhelm, Hör-/ Sprechgarnitur, Atemschutzmaske“ heraus, in der zusätzlich zu Stoßdämpfung, Stichschutz und Helm-Masken-Kombination folgende neue Forderungen für die nächste Helmgeneration enthalten waren: optimierter Stichschutz (Prüfung nach VPAM KDIW 2004 PRÜFRICHTLINIE „Stich- und Schlagschutz“ Anlage 5), erhöhter Flammschutz, reduziertes Gewicht, erweiterter Größenbereich von 46 bis Größe 67 (statt bisher 48−65), verbesserte Hygieneeigenschaften (auswechselbare, waschbare und antibakteriell ausgerüstete Innenausstattung). Damit standen mit der Generation 5 jetzt helmseitig elf Doppelgrößen in drei Kalottengrößen sowie 3 Schutzmaskengrößen zur Verfügung; ein derartig umfangreiches Größenangebot war bei Schutzhelmen für zivile Einsatzzwecke kaum zu finden. Alle drei Kalottengrößen waren leichter als die bisherigen Einsatzhelme der Generation 4 (Schuster, 2015, S. 6−9; Schuberth GmbH, 2015, S. 2). Insbesondere die kleine Helmkalotte kam dem zunehmenden Anteil von Frauen in den Polizeien zugute, eine zügige Einführung wurde daher auch von den Polizeigewerkschaften befürwortet.

Die ersten vier Generationen Bereitschaftspolizeihelme hatten Kinnschutzkappen; ab der dritten Generation waren sie abnehmbar konstruiert, um im Falle der Nutzung als Helm-Masken-Kombination schnell abgenommen werden zu können. Da die Helm-Masken-Kombinationsoption sowie die Einführung der Körperschutzausstattung (KSA) mit Brustpanzerungen verlängerte Visiere wie bei der 2. Generation aus Kompatibilitäts- bzw. Mobilitätsgründen nicht mehr zuließen, wurde nach Möglichkeiten gesucht, den Kinnbereich besser zu schützen. Zeitweise sehr beliebt waren privat beschaffte Kinnschützer aus dem Eishockeysport; ihre Schutzfunktion war jedoch zweifelhaft, aber da sie ein Teil des Gesichts der Einsatzkräfte verdeckten, waren sie beliebt und werden teilweise sogar noch bis heute eingesetzt. Dies wurde in der Richtlinienarbeit bereits früh erkannt; so heißt es in den Änderungsvorschlägen mit Bearbeitungsvermerken zum TR-Entwurf Stand Juni 2006 auf den Seiten 6−7: „Der abnehmbare Kinnschutz ist regelmäßig mit dem Kinngurt verbunden. Alle Normen, nicht zuletzt die ECE 22 in allen Revisionen von 03 bis 05, verbieten einen Kinnschutz in Kombination mit dem Kinngurt. Letztlich ist die Kinnspitze ein außerordentlich unsicherer Befestigungspunkt für einen Schutzhelm. In der Mehrzahl aller Fälle lässt sich der Einsatzhelm nicht sicher befestigen. Häufig rutscht der Kinngurt mit Kinnschutz nach hinten. Die nächste Frage stellt sich zur Schutzwirkung der zierlichen Kinnschutzkappen, die ohne nennenswerte Polsterung auf der Kinnspitze getragen werden und bestenfalls offene Verletzungen verhindern. Die Schlag-/ Wurfenergie verzehrt regelmäßig der Unterkiefer. Die Form der Kinnschutzkappen birgt zusätzliche Gefahren. Kinnschutzkappen, die noch den Mund mit abdecken und unter der Nase

enden, geben dann auch Schlagenergie nach oben zur Nase ab; ein unnötiges Verletzungspotential ist hier gegeben. Fazit: Die Kombination Kinngurt/Kinnschutz ist äußerst problematisch und sollte einer sicheren Variante mit einem gepolsterten Kinnriemen weichen, der unter dem Kinn ohne Kinnschutz befestigt wird. Der Kinnschutz ist trotz seiner Probleme bei den Beamtinnen und Beamten ein unbedingtes, hoch emotional besetztes Erfordernis. Ein Handeln nach objektiven Gesichtspunkten wird schwer!“

Erst in die Maskenschlösser einsetzbare Kinnbügel brachten ausreichend Schutz, da durch sie die Schlagkraft auf die Kalotte abgeleitet werden konnte. Die breitere Einführung dieses Zubehörs zog sich allerdings hin, da erst verschiedenste Erfahrungen gemacht werden mussten. Die erste Ausführung, ein Kinnteil eines ehemaligen Motocrosshelmes (Schuberth CR), war den Einsatzpsychologen zunächst selbst in der Farbe Weiß zu martialisch/aggressiv. Später wurde es dann in größeren Stückzahlen in mattschwarzer Farbe beschafft. Da der Spritzgusskunststoff jedoch nicht flammhemmend war, wurde dieses Anbauteil von einigen Bundesländern abgelehnt und nicht beschafft. Als nächste Forderung kam eine Abreißvorrichtung hinzu, sodass im Fall des direkten Angriffs auf das Kinnteil das polizeiliche Gegenüber dieses abriss und nicht als Hebel nutzen konnte, um die Einsatzkraft zu Boden zu bringen. Diese Nottrennvorrichtung hatte interessanterweise sogar eine Präventivwirkung: Die 2010 im Internet aus autonomen Quellen stammende, unter dem Tarnnamen „Polizeibericht Berlin 2010“ aufgetauchte Schwachstellenanalyse der Berliner Polizeikräfte stellte dazu fest: „Der Kinnbügel ist nur sporadisch im Einsatz; er verfügt über einen Notverschluss, damit er sich bei zu starker Belastung automatisch vom Helm löst. Darum ist es nicht möglich, jemanden daran zu packen“ (Autonome Gruppen, 2010, S. 90). Als Letztes wurde dann festgestellt, dass das zügige, sichere Herunterlaufen von Stadiontreppen im Tribünenbereich ohne den Sichtbereich nach vorne unten nicht möglich bzw. gefährlich ist. Dies führte letztendlich zu der weltweit einzigartigen Entwicklung eines transparenten Kinnschutzmoduls, das sogar noch faltbar ist, um es im Fall des Nichtgebrauchens in der Seitentasche der Einsatzhose verstauen zu können.

Nun stellte sich die Frage der Zertifizierung des Gesamtsystems: Von den in der TR genannten Prüfstellen waren nur das Zentrum für Sicherheitstechnik der Berufsgenossenschaft der Bauwirtschaft (Prüfstelle für Stoßdämpfung) und die DEKRA EXAM GmbH (Prüfstelle für die Atemschutzmaske sowie das Chemikalienverhalten der Schutzhelme) als Zertifizierungsgesellschaft akkreditiert, beide waren aber aufgrund ihrer unterschiedlichen Prüfspektren keine VPAM-Mitglieder. Nach einem intensiven Austausch zwischen dem Autor und dem damaligen Leiter der VPAM, dem Schweizer Matthias Baumer, damals Teamchef Entwicklung beim Forensischen Institut der Kantons- und Stadtpolizei Zürich, hat die VPAM zeitnah entschieden, das VPAM-Nichtmitglied DEKRA EXAM GmbH als Zertifizierer für polizeiliche Einsatzhelme nach TR 2011 zu akzeptieren. Dadurch konnte am 30.06.2015 erstmalig ein Gesamtsystem nach der TR 2011 zertifiziert werden: Zertifikat DEKRA EXAM GmbH Nr. 8266/15/11, gültig bis 01.06.2020 (Schuberth GmbH, 2015, S. 5). Da das neue Schutzmaskenmodell (AVON HM50) ursprünglich für den CBRN-Schutz von Spezialeinheiten entwickelt worden war, konnte durch die 2-Punkt-Anbindung (Helm-Masken-Kombination gegen Tränengas) und die zusätzliche Tragenetzoption (voller CBRN-Schutz) ein signifikant höheres Schutzniveau erreicht werden. Denn trotz der anfänglichen Einwände einiger Bundesländer aufgrund zwischenzeitlich gesetzlich notwendig gewordener Atemgeräteträgerprüfungen wurde aus einsatztaktischen Gründen bundesweit weiterhin an der Helm-Masken-Kombination festgehalten.

Dieses neue Konzept war so beeindruckend, dass der damalige Chefredakteur der Polizeipraxis, des Technikmagazins der Gewerkschaft der Polizei, Reinhard Kaufmann, 2014 sogar auf der Titelseite urteilte:

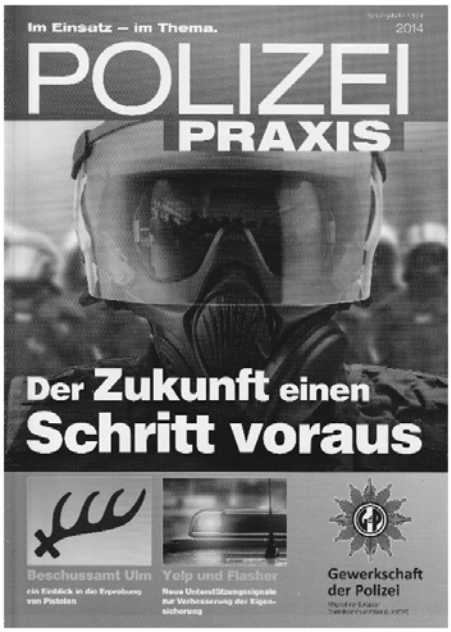


Abb. 6: Titelseite Polizeipraxis 2014

2014 hatte sich auch bereits eine weitere Einsatzmöglichkeit für die Helm-Masken-Kombination ergeben, denn Fußballfans setzten in immer größerem Maße sogenannte Bengalos in Stadioninnenräumen ein. Diese pyrotechnischen Fackeln sind als Seenotrettungsmittel frei verkäuflich. Aufgrund der enormen Hitze (ca. 1.500 °C bis 2.500 °C) stellen sie aber eine besondere Gefährdungsquelle dar, die sofortiges Handeln erfordert. Einer der Polizeieinsatztrainer, der damals deutschlandweit federführend Bekämpfungskonzepte für diese Bedrohung entwickelte, war PHK Gerd Matuszczyk vom Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei Nordrhein-Westfalen (LAFP NRW). Ein spezielles Löschsystem, das direkt in die Öffnung des Bengalos wirken kann, um diesen dauerhaft abzulöschen, wurde mit einer Fachfirma entwickelt. Der Autor durfte parallel bei der Gefährdungsanalyse unterstützen; dabei stellte sich heraus, dass beim Ablöschen von Bengalos auf kürzeste Distanz neben der Eigensicherung zwei weitere Faktoren beachtet werden müssen: Zum einen sind die Abgase des Bengalos derart toxisch, dass die Atemschutzmaske mit entsprechendem Filter angelegt werden muss, und zum anderen müssen die Augen gegen das grelle Licht geschützt werden; hierzu wurde in das Visier modular eine Augenschutzfolie mit optischen Schweißschutzeigenschaften eingebracht.

Zwischenzeitlich wurde dieses Helmsystem nicht nur ergänzt (Kopfgrößenschnellverstellung, optionales Schutzvisier gegen Blendlaser), sondern aktuell deuten sich sogar bereits Weiterentwicklungen an.

So wurde auch diese TR wieder ein Erfolg; sie wurde nach und nach nicht nur in Deutschland, sondern auch in Österreich und der Schweiz und dann in vielen weiteren Ländern Beschaffungsgrundlage.

Bei besonders gewalttägigen Lagen wie z. B. 2010–2012 in Griechenland mit massivem Einsatz von Molotow-Cocktails oder dem arabischen Frühling 2011 wurde von den Einsatzkräften zeitnah die Beschaffung von Helmen nach deutscher TR gefordert und durchgeführt. Arabische Staaten haben später sogar Helme nach TR als Unterstützung an Partnerstaaten verschenkt. Auch in Nordamerika werden derartige Helme bereits erfolgreich beschafft und eingesetzt.

Die Bedeutung des produktspezifischen Fachwissens

Wenn Technische Richtlinien Konstruktionsstände über einen längeren Zeitraum fortschreiben, ist es wichtig, dass das zum Verständnis notwendige technisch/taktische Hintergrundwissen nicht nur bewahrt, sondern weiterhin auch entsprechend ausgebildet wird, um die Schutzausrüstung optimal nutzen zu können. Als einfaches Beispiel kann hier der Sicherheitsverschluss des Kinnriemens gemäß der TR 2011, Punkt 2.2 Schutzhelm dienen. Dieser Notöffnungsverschluss, auch „Ruck-Zuck-Verschluss“ genannt, besteht aus einer geschlossenen (ohne Notöffnungsoption) und einer offenen Triangel (mit Notöffnungsoption), die alternativ am Gegenstück, der sogenannten Platte mit Öse, befestigt werden. Dieses Bauteil ist als einziges in allen Bereitschaftspolizeihelmen der Generationen 1 bis 5 baugleich verbaut:

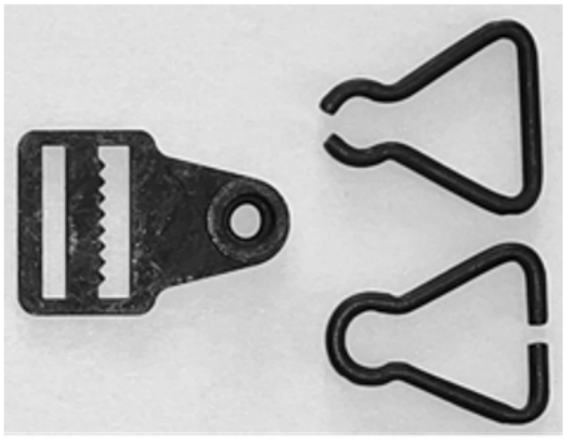


Abb. 7: Platte mit Öse (links), Triangel offen (rechts oben), Triangel geschlossen

In den Änderungsvorschlägen mit Bearbeitungsvermerken zum TR-Entwurf Stand Juni 2006 hieß es allerdings auf Seite 6 hierzu: „Muss der arretierbare „Unsicherheitsverschluss“ noch sein? Der Sicherheitsverschluss soll bei Angriffen auf Beamtinnen und Beamte Verletzungen vermeiden und Fluchtmöglichkeiten eröffnen. Wer soll wann die Entscheidung zur Wahl des richtigen Verschlusses treffen? Die Begründungen zum Sicherheitsverschluss verbieten den arretierbaren Verschluss.“ Hier ist das Wissen um die historische Entstehung und Entwicklung sehr hilfreich für das bessere Verständnis und die Auswahl der Optionen. Die amerikanische Armee hatte 1941 das neue Stahlhelmmodel M1 eingeführt und auf den Schlachtfeldern des 2. Weltkrieges verschiedene Erfahrungen gemacht; der Nachweis findet sich auf Seite 644 von Beyer, J. et al. (1962): “During the course of the North African campaigns in 1943, the rigid hook fastener of the chinstrap was found to be a source of potential danger by remaining intact under the impact of a blast wave resulting from a nearby detonation and thereby jerking the head sharply and violently with the production of fractures or dislocations of the cervical vertebras.

Therefore, it was necessary to redesign the helmet strap with a ball-and-clevis release so that it would remain closed during normal combat activities but would allow for a quick voluntary release or automatic release at pressures considerably below the accepted level of danger. Following extensive tests by ordnance engineers, a new release device was developed which would release at a pull of 15 pounds or more. This device …was standardized in 1944." Durch das Kriegsende und die damit verbundene Produktionseinstellung kam es zu diesem Zeitpunkt nicht mehr zur Einführung des neuen T1-Kinnriemens. Erst bei der Wiederaufnahme der Produktion 1951 aufgrund des Koreakrieges wurde der T1-Kinnriemen flächendeckend eingeführt (Arnold, 1997, S. 191). Da aus politischen Gründen bei der Aufstellung der westdeutschen Bundeswehr 1955/56 − im Gegensatz zum damaligen Bundesgrenzschutz − der Stahlhelm im Design der deutschen Wehrmacht nicht eingeführt werden durfte, wählte man zunächst nach amerikanischem Vorbild den zweiteiligen M1-Helm, mit dem erstmalig ein solcher Sicherheitsverschluss in Deutschland Einzug hielt. In der Nutzung stellte man fest, dass ein solcher Notöffnungsmechanismus weitere Vorteile bot; so kann er bei Schwierigkeiten beim Überwinden von Gewässern das schnelle Ablegen des Helmes ermöglichen, aber insbesondere auch beim Nahkampf bei Angriffen von hinterrücks die Trennung vom Helm ermöglichen, um wieder handlungsfähig zu werden und eine Strangulation durch den Kinnriemen zu verhindern. Nachdem sich das zweiteilige Helmmodell in der Truppe nicht bewährt hatte, wurde ein einteiliges Stahlhelmmodel entwickelt. Dabei wurde der Sicherheitsverschluss im Auftrag des Bundesamtes für Wehrtechnik und Beschaffung (BWB) von der Firma Schuberth überarbeitet; diese Ausführung wird bis heute verwendet. Mit diesem Hintergrundwissen ist es nach wie vor recht einfach zu definieren, wie der Einsatz dieses Sicherheitselementes erfolgen sollte: Alle Einsatzkräfte, die im direkten Kontakt mit dem polizeilichen Gegenüber stehen, sollten die Notöffnungsvariante wählen − **mit einer Ausnahme: beim Einsatz als Helm-Masken-Kombination**, da hier der feste Sitz der Schutzmaske Vorrang hat. Die Auswahl beim Einsatz bei polizeilichen Sonderverwendungen, wie z. B. bei der Polizeireiterstaffel, sollte nach einer entsprechenden internen Gefährdungsanalyse erfolgen.

Frankfurt 1987: Schusswaffeneinsatz während einer Demonstration

Ein tragischer Vorfall wirkt bis heute noch nach, obwohl den meisten Einsatzkräften die historischen Gründe kaum noch bewusst sind: Am 02.11.1987 um ca. 21:05 Uhr schoss ein 33-jähriges Mitglied einer autonomen Gruppe bei Protesten an der Startbahn West des Frankfurter Flughafens mit einer im November 1986 einem Kriminalbeamten abgenommenen Dienstpistole SIG Sauer P6 14 Schüsse aus großer Entfernung auf die Formation der Hessischen Bereitschaftspolizei; der 43-jährige Hundertschaftsführer der IV. Bereitschaftspolizeiabteilung Hanau, PHK Klaus Eichhöfer, und der 23-jährige PM Thorsten Schwalm wurden tödlich getroffen, sieben weitere Beamte zum Teil schwer verletzt (Helmut Brückmann – ein ganz besonderer Mensch ist von uns gegangen, 2022, S. 84). Da der Täter bei späteren Vernehmungen angab, aufgrund der zu dieser Uhrzeit schlechten Lichtverhältnisse zumeist auf die weißen Einsatzhelme gezielt zu haben, kam es zu − teilweise bis heute andauerndem − Unmut bei den Einsatzkräften gegen diese Helmfarbe. Trotzdem ist der ursprünglich als deeskalierend bewertete und von der Innenministerkonferenz für Einsatzhelme vorgegebene Farbton „Weiß" teilweise heute noch im Einsatz. Die hessische Polizei bekam damals zunächst als einzige Polizeiformation die Sondergenehmigung, den Stirnbereich des Einsatzhelmes olivgrün überzulackieren, um die Silhouette des Helmes beim Betrachten von vorne zu ver-

wischen und insbesondere, um den Unmut der Einsatzkräfte zu besänftigen. Zwischenzeitlich haben aber die meisten Bundesländer und der Bund bei den Einsatzhelmen auf dunkle Farbtöne wie Stahlblau (RAL 5011) umgestellt oder verwenden in bestimmten Einsatzlagen zusätzlich noch inhärent flammhemmende Tarnüberzüge für die Einsatzhelme in der Farbe Parisblau (BATEX Technische Textilien GmbH, o. D.).

Obwohl es über die gesamte Nutzungszeit unterschiedliche Hybridkonstruktionen (Bereitschaftspolizeihelm mit zusätzlichem ballistischem Schutz) von verschiedenen Herstellern gab, kam es bisher nicht zur Einführung derartiger Helme, da es die bisher zur Verfügung stehenden Materialien (Stahl/Polycarbonat, Titan, Aramid und Polyethylen) und Fertigungsverfahren nicht zulassen, das zwischenzeitlich erreichte hohe Schutzniveau beider Helmtypen ohne Abstriche in einem Helmmodell zu vereinigen.

Ausblick

Alle diese Erfolge waren nicht zufällig! Dennoch waren die beiden erwähnten Technischen Richtlinien von 2010 und 2011 nicht das Ergebnis eines Regelprozesses, sondern das Ergebnis besonders motivierter Personen, die ihr spezifisches Fachwissen aus Einsatzlagen, der Material- und Verfahrenskunde, dem Prüfwesen und der Verwaltung im Rahmen vager Strukturen aus intrinsischer Motivation zusammengefügt und in Produkte umgesetzt haben, um bedrohungsgerechte, verbesserte Einsatzmittel verfügbar zu machen.

Aktuell findet der dazu auch wichtige Erfahrungsaustausch mit ausländischen Nutzern von TR-gemäßen Einsatzmitteln polizeiintern kaum noch statt; gelegentlich werden zumeist von Herstellern international gesammelte Einsatzerfahrungen in Fachvorträgen vorgestellt und geteilt. Hier ist nun polizeiseitig entschiedenes Handeln – insbesondere im Wissensmanagement – gefordert, um auch zukünftig im Dialog mit Herstellern und Prüfstellen den bestmöglichen Schutz der Einsatzkräfte sicherstellen zu können!

Referenzen

Arnold, C. (1997). Steel Pots – The History of America´s Steel Combat Helmets (1. Aufl.). San Jose, California.

Auergesellschaft GmbH & Schuberth Helme GmbH (1995). Die Helm-Masken-Kombination HMK-P 100 A für Polizei und andere Sicherheitskräfte.

Autonome Gruppen (2010). Polizeibericht Berlin. https://doczz.net/doc/5984-292/autonome-gruppen--polizeibericht-2010

BATEX Technische Textilien GmbH (o. D.). Helmüberzug für Schuberth-Helm P100N. Abgerufen am 28.04.2026 von https://www.batex.de/shop/Helmuberzug-fur-Schuberth-Helm-P100N-p694457183

Beyer, J., Enos, W., & Holmes, R. (1962). Personnel Protective Armor. In J. Coates (Hrsg.), Wound Ballistics. Department of the Army. Abgerufen am 28.04.2026 von https://achh.-army.mil/history/book-wwii-woundblstcs-chapter-11

Busch PROtective Germany GmbH & Co. KG (o. D.). AMP-1 X selected as primary ballistic helmet for the FBI. Abgerufen am 28.04.2026 von https://-busch-protective.com/fbi-ballistic-helmet-contract/

Deutsche Hochschule der Polizei (2009). Programm Workshop der Deutschen Hochschule der Polizei „Durchschusshemmender Helm“ am 01./02. Juli 2009 [Unveröffentlichtes Programm].

Hans, J.-M. (2017). „PTI 2.0“, Das Polizeitechnische Institut, Neuaufbau und Perspektiven. Polizeipraxis, 2017/1, 34–35.

Ferrand, A., & Zaglia, C. (2005). Fire Helmets – Companions in the fight against fire, Saint-Amand-Montrond.

Forschungs- und Entwicklungsstelle für Polizeitechnik (1982). Programm zur Ermittlung von Prüfkriterien von Schutzhelmen [Unveröffentlichtes Programm].

Artikeltitel „Harter Aufschlag! Große Genauigkeit!“ Chaoten-Kampfmittel Präzisionsschleuder: Gefährlich wie Schusswaffen (1986). Der Spiegel, Nr. 30, 28.

Helmut Brückmann – ein ganz besonderer Mensch ist von uns gegangen (2022). Der Sicherheitsdienst, 2/2022, 83–85. Abgerufen am 28.04.2026 von https://www.dersicherheitsdienst.de/e-paper/2022-03/84/

Herminghaus, T. W. (1982), Feuerwehrhelme – Eine Entwicklungsgeschichte (1. Aufl.), Hanau.

Kienle, O., (1968). Der Helm − Eine zeitgemäße Betrachtung. Fachzeitschrift für Verkehrs- Kraftfahr- Fernmelde- Waffenwesen- und ABC-Schutz der Polizei (heute pvt POLIZEI VERKEHR + TECHNIK), 11/1968, 457.

Polizei-Führungsakademie, Forschungs- und Entwicklungsstelle für Polizeitechnik (1982). Anforderungen und Prüfvorschrift für „beschusshemmenden Kopfschutz“ [Unveröffentlichte Vorschrift].

Polizei-Führungsakademie, Polizeitechnisches Institut (2004). Zertifikat Nr. SH-AM 01 04 [Unveröffentlichtes Zertifikat].

Polizeitechnisches Institut der Deutschen Hochschule der Polizei (2006). Entwurf Technische Richtlinie (TR) für ein modular aufgebautes System - Schutzhelm, Hör-/Sprechgarnitur, Atemschutzmaske - [Unveröffentlichter Entwurf].

Polizeitechnisches Institut der Deutschen Hochschule der Polizei (2008). Entwurf Technische Richtlinie (TR) für ein modular aufgebautes System - Schutzhelm, Hör-/Sprechgarnitur, Atemschutzmaske - [Unveröffentlichter Entwurf].

Polizeitechnisches Institut der Deutschen Hochschule der Polizei (2010). Technische Richtlinie (TR) Gesamtsystem „Ballistischer Helm“. Abgerufen am 28.04.2026 von https://www.dhpol.-de/microsite/pti/medien/downloads/richtlinien/technische-richtlinien/einsatzhelm/TR-Helm-ballistisch_05-2010.pdf

Polizeitechnisches Institut der Deutschen Hochschule der Polizei (2011). Technische Richtlinie (TR) für ein modular aufgebautes System - Schutzhelm, Hör-/Sprechgarnitur, Atemschutzmaske -. Abgerufen am 28.04.2026 von https://-www.dhpol.de/-microsite/pti/medien/downloads/richtlinien/technische-richtlinien/einsatzhelm/-TR_modular_aufgebautes_System_Schutzhelm.pdf

Radecke, E. (1981). Geschichte des Polizei-Tschakos (1. Aufl.). Hilden.

Schröder, W. (2005a). Fortschritte und Vorschriften bei der Einsatzbekleidung. POLIZEI-heute, Januar/Februar 2005, 27−29.

Schröder, W. (2005b). Schwer entflammbar und mit Feuchtemanagement. POLIZEI-heute, Mai/Juni 2005, 109−111.

Schuberth GmbH (2015). HMK150 Helm-Masken-Kombination.

Schuster, L. (2015), Die Helm-Maskenkombination HMK150 – Einsatztechnik für die Zukunft von Profis für Profis, Polizeipraxis, 2014, 6−9. Abgerufen am 28.04.2026 von https://www.polizeipraxis.de/startseite/news-detailseite/artikel-/die-helm-maskenkombination-hmk.html

Technische Kommission des Arbeitskreises II (1992). Technische Richtlinie (TR) für ein modular aufgebautes System - Schutzhelm, Hör-/Sprechgarnitur, Atemschutzmaske -. Unterausschuss Führungs- und Einsatzmittel des Arbeitskreises II (1997). Technische Richtlinie (TR) Durchschusshemmender Helm.

Vereinigung der Prüfstellen für angriffshemmende Materialien und Konstruktionen (2011). KDIW 2004 Stich- und Schlagschutz - Anforderungen, Klassifizierung und Prüfverfahren -. Abgerufen am 28.04.2026 von https://www.vpam.eu/-wp-content/uploads/2022/12/20110518_II_KDIW2004.pdf

Vereinigung der Prüfstellen für angriffshemmende Materialien und Konstruktionen (2017). HVN 2009 Durchschusshemmender Helm, Visier und Nackenschutz - Anforderungen, Klassifizierungen und Prüfverfahren -. Abgerufen am 28.04.2026 von https://www.vpam.eu/wp-content/uploads/2022/12/20170404-_II_HVN2009.pdf

Artikeltitel „Wenn der erste Demonstrant schießt…“ (1986). *Der Spiegel*, Nr. 30, 26–50.

Zahn, C. (1986). Besprechungsprotokoll mit dem Inspekteur der Bereitschaftspolizeien der Länder im Bundesministerium des Innern H.-J. Gebauer vom 17.07.1986 [Unveröffentlichtes Besprechungsprotokoll].

Technologische Transformation und institutionelle Anpassung – Das Polizeitechnische Institut im digitalen Zeitalter

Wilfried Honekamp

Das Polizeitechnische Institut (PTI) der Deutschen Hochschule der Polizei (DHPol) nimmt innerhalb der Sicherheitsarchitektur der Bundesrepublik Deutschland eine zentrale Rolle bei der Bewertung, Koordination und Weiterentwicklung polizeilicher Technik ein. In den vergangenen fünf Jahrzehnten hat das Institut eine kontinuierliche Entwicklung durchlaufen, die von einer primär administrativ-fachtechnischen Prüfstelle hin zu einer Einrichtung führte, deren Aufgabenfeld sich deutlich erweitert hat und heute in vielfältige, zunehmend digital geprägte Technologiezusammenhänge eingebunden ist (Kötter, 1995; PFA, 1998; PTI, 2026). Während die Anfänge des Instituts im Jahr 1974 als „Forschungs- und Entwicklungsstelle für Polizeitechnik“ (FEStPt) noch stark durch die Erprobung und Standardisierung physischer Einsatzmittel geprägt waren (Kötter, 1995), ist das heutige Aufgabenspektrum wesentlich durch digitale Systeme, Datenverarbeitung und vernetzte Anwendungen bestimmt (PTI, 2021, 2025). Diese Entwicklung markiert den Übergang von der Bewertung einzelner materieller Einsatzmittel hin zur Befassung mit vernetzten digitalen Technologien, Datenarchitekturen, mobilen Endgeräten, Sensorik und Anwendungen der Künstlichen Intelligenz (KI) (PTI, 2019; PTI, 2026). In diesem Prozess hat sich das PTI von einer administrativ orientierten Instanz, die primär nach klassischen Verwaltungslogiken agierte, zu einer zentralen Schnittstelle zwischen Forschung, Industrie, Verwaltung und operativer Polizeipraxis entwickelt. Technische Expertise ist damit heute stärker als früher mit rechtlichen, ethischen und organisatorischen Anforderungen verbunden (PTI, 2021, 2025, 2026).

Die institutionelle Anpassung, die ab dem Jahr 2016 mit dem Konzept „PTI 2.0“ und der Einführung einer agilen Matrix-Organisation im Jahr 2018 eingeleitet wurde (Hans, 2017; PTI, 2019), gipfelte im Zeitraum 2023/2024 in der Umwandlung zu einer wissenschaftlichen Einrichtung. Diese Neuausrichtung unterstreicht die zunehmende Bedeutung, technologische Entwicklungen nicht mehr nur zu bewerten, sondern sie auch durch eigene Forschungsaktivitäten zu begleiten. Das PTI übernimmt heute verstärkt Aufgaben im Bereich des strategischen Technologieradars, der Beratung nationaler und internationaler Gremien sowie des Aufbaus zentraler Wissensdatenbanken für die Polizeien des Bundes und der Länder (DHPol, 2025; Klingelhöfer & Honekamp, 2025). Ziel dieses Beitrags ist es, diesen Transformationsprozess von den Ursprüngen bis hin zum modernen Forschungsinstitut im digitalen Zeitalter darzustellen. Dabei wird aufgezeigt, wie das Institut durch die kontinuierliche Anpassung seiner Strukturen und Aufgabenbereiche, von der klassischen Richtlinienarbeit bis hin zur Bewertung KI-basierter Anwendungen, die polizeiliche Handlungsfähigkeit angesichts hybrider Bedrohungen und des technologischen Wandels langfristig sichert (PTI, 2026).

Die Ursprünge: Von der FEStPt zum PTI (1974–1999)

Die Gründung der „Forschungs- und Entwicklungsstelle für Polizeitechnik“ (FEStPt) im Jahr 1974 war eine direkte Reaktion auf die verschärfte Sicherheitslage in der Bundesrepublik Deutschland zu Beginn der 1970er Jahre. Insbesondere die terroristischen Aktivitäten der Ro-

ten Armee Fraktion, gewalttätige Demonstrationen an Kernkraftwerken sowie neue Herausforderungen durch das aufkommende Fußballrowdytum und schwere Katastrophenlagen machten eine verstärkte Zusammenarbeit und technische Unterstützung der Polizeien des Bundes und der Länder erforderlich. Es bestand die dringende Notwendigkeit, eine zentrale Koordinierungs- und Servicestelle zu schaffen, um die technische Handlungsfähigkeit der Sicherheitsbehörden durch Kompatibilität und Standardisierung sicherzustellen. Um diese bundeseinheitlichen Standards zu gewährleisten, wurde die FEStPt institutionell in der damaligen Polizei-Führungsakademie (PFA) in Münster-Hiltrup verankert. Diese Standortwahl erfolgte mit ausdrücklicher Zustimmung aller Länder und des Bundes. Die Finanzierung der Einrichtung wurde durch eine gemeinschaftliche Kostenteilung nach dem Königsteiner Schlüssel realisiert. Damit fungierte die FEStPt als zentrale fachtechnische Dienststelle, die Leistungsmerkmale für Führungs- und Einsatzmittel definierte und durch die Erarbeitung Technischer Richtlinien (TR) sicherstellte, dass polizeiliche Ausrüstung bundesweit einheitlichen Qualitäts- und Sicherheitsstandards entsprach (Kötter, 1995; PFA, 1998). Auch personell war die FEStPt zunächst auf eine fachlich breit angelegte Bearbeitung unterschiedlicher Technikfelder ausgerichtet. Das Organigramm aus dem Jahr 1978 weist fünf Dezernate aus. Unter Einbeziehung von Leitung, Sachbearbeitung, Schreibdienst und technischem Dienst waren zu diesem Zeitpunkt rund zwei Dutzend Personalstellen vorgesehen. Mitte der 1990er Jahre schrumpfte der Personalkörper aufgrund personeller Engpässe infolge von Wiederbesetzungssperren allerdings deutlich.

Schult (1985) verdeutlicht, dass die Aufgabe der FEStPt von Beginn an nicht auf abstrakte Richtlinienarbeit beschränkt war. Er beschreibt, dass die Forschungs- und Entwicklungsstelle für Polizeitechnik im Jahr 1975 ihre Arbeit aufnahm und zum 1. Januar 1977 Bestandteil des Fachbereichs Polizeitechnik wurde. Zu ihren frühen Arbeitsschwerpunkten gehörten unter anderem Untersuchungen zu Schutzwesten, Reizstoffen, polizeilichen Datenfunkverfahren, Kraftfahrzeugen als Antennen, Führungs- und Einsatzmitteln zur Kommunikation sowie technischen Sicherungsmaßnahmen für kerntechnische Einrichtungen. Steffen (1995) verweist darauf, dass die FEStPt zugleich als Geschäftsstelle der Technischen Kommission fungierte. Zu den frühen Arbeitsergebnissen zählte unter anderem die technische Richtlinie „Funkmeldesystem“; das in der Festschrift abgebildete Einbausystem der Funkausstattung eines Streifenwagens verweist zudem auf die technische Richtlinie „Funkstreifenwagen“.

Polizeispezifische Forschung und Entwicklung wurden bereits früh als eigenständige Voraussetzung für künftige Führungs- und Einsatzmittel verstanden. Das dokumentierte Themenspektrum reichte von wissensbasierten Systemen und Verkehrsunfallaufnahme bei Fahrzeugen mit Antiblockiersystem über digitale Sprech- und Datenfunksysteme bis hin zu Irritations- und Schockmitteln (Kuratorium der Polizei-Führungsakademie, 1993). Einzelne Forschungsaufträge verdeutlichen zudem die große thematische Spannweite dieser Arbeit: Sie reichte von toxikologischen Untersuchungsverfahren im Speichel und der Erprobung von Atemalkoholmessgeräten über Fragen der ballistischen Schutzwirkung und des Langzeitverhaltens von Schutzwesten bis hin zu frühen Untersuchungen sprachgesteuerter Dateneingabe in polizeilichen Anwendungen.

Der frühe digitale Bezug zeigt sich besonders im Informations- und Kommunikationswesen. Bereits vor der Umwandlung der FEStPt in das PTI wurden technische Anforderungen an Fernseh-Funkanlagen, Fernseh-Richtfunkanlagen und digitale Fernsehbildübertragung for-

muliert. Die 1998 vorliegende Richtlinie zur digitalen Fernsehbildübertragung reagierte auf Schwächen analoger Systeme, insbesondere fehlenden Schutz vor unberechtigtem Mitsehen und Mithören, begrenzte Übertragungskanäle sowie fehlende Datenkanäle für Fernwirken und Rückmeldungen (PTI, 1998b). Parallel dazu wurden im Bereich zukünftiger digitaler Funksysteme Fragen der elektromagnetischen Umweltverträglichkeit und BOS-spezifischer Kommunikationsanforderungen untersucht (Bahr et al., 1997; Kühnberger, 1997). Damit war die spätere digitale Ausrichtung des PTI bereits in der späten FEStPt-Phase technisch vorbereitet.

In den zwei Jahrzehnten festigte die FEStPt ihre Rolle als unverzichtbare Schnittstelle zwischen der polizeilichen Praxis und der technischen Entwicklung. Ein Meilenstein in der Geschichte der Einrichtung wurde im Jahr 1997 erreicht: Auf Grundlage umfassender Analysen zur zukünftigen Aufgabenstellung beschloss das Kuratorium der PFA im Oktober 1997 die Umwandlung der FEStPt in das Polizeitechnische Institut (PFA, 1998; Kötter, 1995). Diese organisatorische Neuausrichtung diente dem Ziel, zukunftsfähige Strukturen zu schaffen, die über die reine fachtechnische Prüfung hinausgingen. Das neue Aufgabenprofil des PTI umfasste bereits damals die Bereiche Informationsstelle für Polizeitechnik, Forschung, fachtechnische Beratung und Unterstützung von Bund und Ländern sowie die Beteiligung an der Lehre. Die endgültige Etablierung des Instituts unter seinem heutigen Namen im Frühjahr 1998 markierte den Übergang zu einer modernen Dienstleistungseinrichtung für die deutsche Polizei (PFA, 1998).

Das PTI an der Schwelle zum digitalen Zeitalter (2000–2015)

Um das Jahr 2000 war die institutionelle Rolle des Instituts als fachtechnische Zentralstelle innerhalb der deutschen Sicherheitsarchitektur fest etabliert. Der Fokus der Tätigkeit lag primär auf der Erprobung, Bewertung und Standardisierung polizeilicher Führungs- und Einsatzmittel, wobei das PTI sicherstellte, dass technische Innovationen der Industrie den operativen Anforderungen der Praxis entsprachen. Zu den traditionellen Kernaufgaben dieser Ära gehörten die Weiterentwicklung der Fahrzeugtechnik, das Waffen- und Gerätewesen sowie die kontinuierliche Verbesserung der Schutzausstattung für Einsatzkräfte. Ein wesentlicher Pfeiler der Institutsarbeit war zudem die Funktion als Zentralstelle für Sicherungstechnik, die insbesondere den Schutz kerntechnischer Einrichtungen und den Transport radioaktiver Stoffe umfasste. In dieser Zeitspanne wurde Technik im polizeilichen Kontext weitgehend als abgeschlossenes, physisches Einsatzmittel verstanden. Die damit verbundenen Beschaffungsprozesse folgten stabilen, klassischen Verwaltungslogiken, und die technologischen Innovationszyklen waren im Vergleich zur heutigen Dynamik eher langfristig orientiert.

Bereits an der Schwelle zum digitalen Zeitalter zeichnete sich eine grundlegende Verschiebung der Anforderungen ab, da die Informations- und Kommunikationstechnik das bisherige Verständnis von Polizeitechnik erweiterte. In Bänden der Schriftenreihe der Polizeiführungsakademie wird dargestellt, dass um die Jahrtausendwende klassische Themen der Einsatztechnik und neue digitale Anwendungsfelder parallel bearbeitet wurden. Der Band Aktuelle Problemstellungen im Bereich der Polizeitechnik bündelt unter anderem Beiträge zu UMTS-Mobilfunknetzen und digitalen Funk-Kommunikationssystemen, Gesundheitsrisiken durch Funkanwendungen, Schutzausstattungen, Einsatzfahrzeugen, biometrischer Identifikation sowie europäischen Kooperationsformen im Bereich der Polizeitechnik. Der Band Polizei-

technik im Wandel erweiterte dieses Spektrum um Themen wie Digitalfunk, digitale Fotografie und Videografie, Authentisierung digitaler Bilder, das Publizieren bestehender Dokumente im World Wide Web sowie vernetzte Informationen. Damit lässt sich erkennen, dass die Digitalisierung polizeilicher Technik als fachtechnische Herausforderung wahrgenommen wurde, ohne dass klassische Felder wie Schutzausstattung, Fahrzeuge oder technische Standardisierung an Bedeutung verloren (Kuratorium der Polizei-Führungsakademie, 2000, 2002).

Die fachtechnische Auseinandersetzung mit digitalen Kommunikationssystemen zeigte sich auch in Stellungnahmen zu öffentlichen Mobilfunknetzen. Das PTI prüfte bereits vor der flächendeckenden Einführung moderner mobiler Datendienste, ob GSM- und später UMTS-Netze die taktisch-betrieblichen Anforderungen der BOS erfüllen könnten. Trotz der absehbaren Leistungssteigerungen im Bereich mobiler Datenübertragung kam das PTI zu dem Ergebnis, dass öffentliche Mobilfunknetze wegen ihrer telefonorientierten Architektur zentrale Anforderungen des professionellen Betriebsfunks, insbesondere betriebsfunktypische Gruppenkommunikation, dynamisches Gruppenmanagement, Direct Mode und netzseitig abgesicherte Kommunikationsstrukturen, nicht vollständig erfüllen konnten (PTI, 1998a, 2000).

Diese Entwicklung wurde auch durch gemeinsam mit dem Bundeskriminalamt erstellte Berichte zu neuen Technologien und ihren Auswirkungen auf den Polizeibereich begleitet. An ihrem Themenspektrum lässt sich erkennen, dass sich die polizeitechnische Aufmerksamkeit in dieser Phase deutlich ausweitete: Standen zu Beginn der 2000er Jahre noch Digitalfunk, öffentliche Mobilfunknetze, Internetnutzung, Kryptografie, Telekommunikationsüberwachung, GPS, Biometrie und digitale Bildverarbeitung im Vordergrund, rückten später zunehmend Software-Agenten, autarke Mikrosysteme, intelligente Videoanalyse, 3D-Gesichtserkennung, Robotik, 3D-Druck, Augmented Reality, Human Language Technology, De-Anonymisierung, ID-Matching sowie Smart-Home- und Smart-Grid-Anwendungen in den Blick.

Ein früher Meilenstein dieser digitalen Transformation war die Bereitstellung des Portals PTI-Online im Jahr 2002, über welches das Institut begann, technisches Wissen, Richtlinien und Marktanalysen digital für die Polizeien des Bundes und der Länder verfügbar zu machen (Klingelhöfer & Honekamp, 2025). Diese Phase markierte den Beginn einer Entwicklung hin zu einem Akteur in komplexen soziotechnischen Systemen, in denen technische Expertise verstärkt mit rechtlichen und organisatorischen Anforderungen verzahnt werden musste.

Die Arbeit musste allerdings mit reduzierten personellen Kapazitäten bewältigt werden. Das PTI verfügte formal noch über 13 Personalstellen. Tatsächlich waren zeitweilig nur neun Mitarbeitende beschäftigt. Vor Umsetzung des Konzepts „PTI 2.0“ waren nach Hans (2017) lediglich zwei Stellen zur Aufgabenerledigung verblieben.

Strategische Neuausrichtung: „PTI 2.0“ (2016–2022)

Ende 2016 begann eine umfassende strategische Neuausrichtung, die das Institut unter dem Leitbild „PTI 2.0“ als zentralen „Single Point of Contact“ für alle technologischen Belange der deutschen Polizeien positionierte (Hans, 2017; PTI, 2018). Ziel dieser Reorganisation war es, eine zentrale Informationsbörse zu schaffen, die technisches Expertenwissen bündelt, Erfahrungen aus Pilotprojekten vernetzt und synergetisch für Bund und Länder nutzbar macht

(Hans, 2017; PTI, 2023). Ein wesentlicher Pfeiler dieser Transformation war der strukturelle Wandel im Jahr 2018 hin zu einer agilen Matrix-Organisation (PTI, 2019). Die Einführung flacher Hierarchien und das Aufgeben starrer Sachbearbeiterpositionen zugunsten von zielorientiertem Projektdenken strebte eine flexiblere und projektorientierte Bearbeitung technischer Fragestellungen an und wurde in den Folgejahren fortgeführt. Diese Organisationsform wurde in den folgenden Jahresberichten als bewährt beschrieben (PTI, 2019, 2020, 2021). Die Neuausrichtung ging zugleich mit einer deutlich schlankeren personellen Zielstruktur einher. Vorgesehen war ein Kernteam aus der Institutsleitung und fünf weiteren Mitarbeitenden. Die Personalgewinnung verzögerte sich zunächst. Bis zum Juni 2018 waren jedoch alle sechs vorgesehenen Stellen besetzt. Damit verfügte das Institut über die personelle Basis, um die Aufgaben in den Bereichen Waffen- und Schutzausstattung, Fahrzeugtechnik, Verkehrsüberwachung und digital geprägte Einsatztechnik projektorientiert zu bearbeiten (PTI, 2019).

Im Bereich der Digitalisierung setzte das Institut neue Schwerpunkte und etablierte Fachformate wie die Konferenz „Verkehrsüberwachung zukunftsorientiert entwickeln“, um Innovationen bei der Drogendetektion und automatisierten Überwachungssystemen zu forcieren (PTI, 2021, 2023). Parallel dazu rückten technologische Felder wie Automotive IT und die Integration mobiler Endgeräte in das polizeiliche Einsatzumfeld in den Fokus der strategischen Arbeit (PTI, 2019). Die zunehmende Internationalisierung der Polizeitechnik wurde durch die Übernahme einer Rolle im European Network of Law Enforcement Technology Services (ENLETS) reflektiert, in dem das PTI als nationaler Kontaktpunkt (NCP) für Deutschland fungiert. In dieser Funktion koordiniert das Institut den Austausch zwischen deutschen Experten und europäischen Arbeitsgruppen, um nationale Bedarfe in europäische Standardisierungsprozesse einzubringen und internationale Trends frühzeitig als technologisches Frühwarnsystem zu identifizieren (Honekamp & Sormes, 2026; PTI, 2020, 2023).

Ein Fortschritt im Informationsmanagement gelang mit dem Relaunch der Plattform „PTI-Online“ im April 2019. Die neue technische Basis ermöglichte eine verbesserte Bereitstellung von Richtlinien und Forschungsberichten für die polizeiliche Fachöffentlichkeit (PTI, 2020). Zeitgleich wurden die ersten Konzepte für eine passwortgeschützte PTI-Datenbank initiiert. Diese Datenbank sollte als zentrales Wissensmanagement-Tool dienen, um technische Informationen, Leistungsbeschreibungen und Erfahrungsberichte bundesweit abrufbar zu machen und so Doppelarbeiten bei Beschaffungsvorhaben zu vermeiden (Klingelhöfer & Honekamp, 2025; PTI, 2022). Obwohl die Umsetzung aufgrund technischer Limitierungen externer Dienstleister im Jahr 2022 verzögert wurde, bildete diese Phase das konzeptionelle Fundament für die spätere Erreichung digitaler Souveränität (PTI, 2023).

Transformation zum wissenschaftlichen Institut (2023–heute)

Im Zeitraum 2023/2024 erreichte das Polizeitechnische Institut (PTI) einen neuen Meilenstein seiner institutionellen Entwicklung. Mit dem Inkrafttreten der neuen Institutsordnung am 14. Januar 2025 wurde das PTI gemäß der Grundordnung der Deutschen Hochschule der Polizei offiziell als wissenschaftliche Einrichtung innerhalb der DHPol anerkannt. Diese formale Aufwertung markiert den Übergang von einer primär unterstützenden Serviceeinheit hin zu einer Einrichtung, die neben ihren bisherigen Aufgaben auch die Erforschung der Polizeitechnik als eigenständiges Aufgabenfeld wahrnimmt (DHPol, 2025). Während das

PTI zuvor als fachtechnische Einrichtung mit primär administrativ-polizeilicher Prägung organisiert war und durch Polizeivollzugsbeamte geführt wurde, ist es nun strukturell in die Hochschulorganisation integriert und wird von einer Professur geleitet. Diese Transformation betrifft weniger die vollständige Ablösung bisheriger Aufgaben als vielmehr deren Einbettung in einen wissenschaftlichen Kontext. Die klassischen Funktionen, insbesondere Informationsstelle, Richtlinienarbeit und fachtechnische Beratung, bleiben erhalten, werden jedoch um Forschungsaktivitäten ergänzt und in eine hochschulische Struktur überführt.

Das Forschungsprofil des PTI umfasst heute Projekte wie den Aufbau eines Technologieradars zur Früherkennung technologischer Trends (PTI, 2025). Weitere Schwerpunkte bilden die Untersuchung der Auswirkungen von KI auf die polizeiliche Praxis sowie innovative Ansätze im Bereich Augmented Reality, etwa durch die Integration digitaler Informationen in Einsatzhelme (Honekamp & Klingelhöfer, 2026; PTI, 2026). Mit dem Projekt SAFEPol, das sich der automatisierten Freigabe von Einsatzrouten widmet, ist das PTI zudem in ein drittmittelgefördertes Konsortialprojekt eingebunden (PTI, 2026). Vor dem Hintergrund der Transformation zur wissenschaftlichen Einrichtung zeigt SAFEPol, wie sich die erweiterten Forschungsaufgaben des PTI in anwendungsorientierten Verbundprojekten konkretisieren.

Im Sinne der digitalen Souveränität vollzog das Institut auch einen strategischen Richtungswechsel beim Wissensmanagement. Nachdem externe Vergaben nicht die gewünschten Ergebnisse lieferten, entschied sich das PTI für den eigenverantwortlichen Aufbau der PTI-Datenbank auf Basis des modernen Kollaborationstools Confluence innerhalb des Polizei-Netzwerks Extrapol. Dieses System dient als zentrale Wissensplattform, um technische Richtlinien, Erfahrungsberichte, Statistiken und Leistungsbeschreibungen bundesweit sicher verfügbar zu machen und den Wissenstransfer zwischen den Polizeien des Bundes und der Länder nachhaltig zu sichern (Klingelhöfer & Honekamp, 2025; PTI, 2025).

Die Verbindung von Forschung und Praxis spiegelt sich zudem in der Lehre und dem Transfer wider. Technologische Themen sind heute integraler Bestandteil der Masterstudiengänge der DHPol, wobei Module zu KI im polizeilichen Umfeld oder Lehrveranstaltungen zur strategischen Verkehrsüberwachung direkt vom PTI durchgeführt werden (PTI, 2025; PTI, 2026). Durch die Betreuung von Masterarbeiten und die Einbindung von Studierenden in aktuelle Forschungsprojekte stellt das PTI sicher, dass wissenschaftliche Erkenntnisse unmittelbar in die Qualifizierung polizeilicher Führungskräfte einfließen (DHPol, 2025; PTI, 2025).

Integrative Technologiegovernance und Zukunftskonzept „PTI 2027“

Die gegenwärtige Entwicklungsphase des Polizeitechnischen Instituts ist durch eine Verschiebung des Aufgabenprofils hin zu einer integrativen Technologiegovernance gekennzeichnet, die als koordinierte Steuerung und Gestaltung technologischer Entwicklungen unter Einbezug unterschiedlicher Akteure und Regelungsmechanismen verstanden wird (OECD, 2023). In einer Zeit, in der Technik als dynamisches, datenbasiertes und vernetztes System begriffen wird, reicht eine rein fachtechnische Bewertung der Ausrüstung nicht mehr aus. Vielmehr führt das PTI heute die Dimensionen der technischen Leistungsfähigkeit, der rechtlichen Zulässigkeit, der ethischen Vertretbarkeit und der organisatorischen Implementierbarkeit systematisch zusammen. Dieser ganzheitliche Ansatz ist notwendig, um die po-

lizeiliche Handlungsfähigkeit in hochkomplexen soziotechnischen Systemen dauerhaft zu gewährleisten und technologische Innovationen verantwortungsbewusst in den Dienstalltag zu integrieren. Einen gewichtigen strategischen Rahmen für diese Transformation bildet das Zukunftskonzept „PTI 2027“, das zu Beginn des Jahres 2025 initiiert wurde. Angesichts zunehmender hybrider Bedrohungen und der technologischen Dynamik zielt das Konzept auf eine Stärkung der Kernbereiche „Waffen und Schutzausstattung“, „Informations- und Kommunikationstechnik“ sowie den gezielten Ausbau der Forschungsaktivitäten ab. Ziel ist es, die Leistungsfähigkeit des Instituts präzise an die wachsenden Bedarfe der Polizeien der Länder und des Bundes anzupassen. Hierbei ist auch die nachhaltige personelle Qualifizierung von besonderer Bedeutung: Ein spezielles Fortbildungskonzept ermöglicht es den Ländern, Personal an das PTI abzuordnen, um dort tiefgreifende Expertise in neuen Technologiefeldern zu sammeln und diese Kompetenzen anschließend als Multiplikatoren in die Heimatorganisationen zurückzutragen (PTI, 2026).

Ein besonderer Fokus der strategischen Arbeit liegt auf der Erhöhung der Resilienz und Cybersicherheit polizeilicher Infrastrukturen. Das PTI übernimmt hierbei eine tragende Funktion in der Aus- und Fortbildung von Führungskräften zur Bewertung KI-basierter Anwendungen, um Potenziale für die Kriminalitätsbekämpfung zu erschließen und technologische Risiken für polizeiliche Systeme zu minimieren (PTI, 2025; PTI, 2026). Dies umfasst die Untersuchung der Auswirkungen von KI auf die polizeiliche Aus- und Fortbildung sowie die Forschung an KI-gestützten Verfahren zur effizienten Informationsgewinnung aus kriminalpolizeilichen Massendaten (PTI, 2026). Durch Forschung zum Aufbau eines systematischen Technologieradars hat das Institut zudem die Grundlagen für ein technologisches Frühwarnsystem ermittelt. Trends wie Augmented Reality oder automatisierte Videoanalyse konnten rechtzeitig identifiziert und strategisch bewertet werden (Morgenstern & Honekamp, 2024; PTI, 2025; PTI, 2026). Damit trägt das PTI zum Schutz kritischer polizeilicher Infrastrukturen sowie zur digitalen Souveränität der deutschen Sicherheitsbehörden im digitalen Zeitalter bei (Klingelhöfer & Honekamp, 2025).

Schlussfolgerungen

Die Entwicklung des PTI veranschaulicht, dass polizeiliche Technik seit Beginn des 21. Jahrhunderts nicht mehr allein als Ausstattung, Gerät oder Einsatzmittel verstanden werden kann. Mit der Digitalisierung polizeilicher Aufgabenfelder verschiebt sich der institutionelle Bedarf von der Prüfung einzelner technischer Produkte hin zur Bewertung komplexer soziotechnischer Systeme. Für das PTI bedeutet dies eine Erweiterung seines klassischen Standardisierungs- und Beratungsauftrags: Neben technische Leistungsfähigkeit treten Fragen der Datenverarbeitung, Interoperabilität, rechtlichen Zulässigkeit, organisatorischen Implementierung und wissenschaftlichen Evaluation. Diese Verschiebung erklärt auch die institutionelle Neuausrichtung des Instituts. Die Entwicklung von PTI 2.0, Matrixorganisation, PTI-Datenbank, Technologieradar und wissenschaftlicher Einbindung ist weniger als Bruch mit der bisherigen Aufgabenwahrnehmung zu verstehen, sondern vielmehr als Anpassung an veränderte Anforderungen der Polizeien des Bundes und der Länder. Das PTI bleibt damit eine fachtechnische Koordinierungsstelle, übernimmt aber zunehmend die Funktion eines Wissens-, Transfer- und Forschungsknotens zwischen Polizeipraxis, Hochschule, Verwaltung und Technologieentwicklung.

Für die Polizeitechnik im 21. Jahrhundert ist diese Entwicklung exemplarisch. Sie zeigt, dass technische Handlungsfähigkeit durch die dauerhafte Fähigkeit entsteht, technologische Entwicklungen frühzeitig zu erkennen, fachlich zu bewerten, rechtlich und organisatorisch einzuordnen und in die polizeiliche Praxis zurückzukoppeln. Die künftige Bedeutung des PTI wird daher maßgeblich davon abhängen, ob es gelingt, klassische Richtlinienarbeit, anwendungsorientierte Forschung, Wissensmanagement und strategische Technologiebeobachtung dauerhaft miteinander zu verbinden.

Referenzen

Bahr, A., Pan, S.-G., & Rebmann, B. (1997). Messtechnische Untersuchung der elektromagnetischen Umweltverträglichkeit von Funksystemen der Polizei. Institut für Mobil- und Satellitenfunktechnik GmbH.

DHPol. (2025). Institutsordnung des Polizeitechnischen Instituts der Deutschen Hochschule der Polizei. Amtliche Bekanntmachung, (23), 247–254.

Hans, J.-M. (2017). „PTI 2.0“ Das Polizeitechnische Institut – Neuaufbau und Perspektiven. Polizei Verkehr + Technik (pvt), 62(2), 15.

Honekamp, W., & Klingelhöfer, M. (2026). Polizeiliche Praxis als Motor der Sicherheitsforschung. Polizei Verkehr + Technik (pvt), 71(3), 9–11.

Honekamp, W., & Sormes, M. (2026). Technologie verbindet – das Netzwerk ENLETS und seine Bedeutung für die Polizeiarbeit. Polizei Verkehr + Technik (pvt), 71(1), 8–10.

Klingelhöfer, M., & Honekamp, W. (2025). Die PTI-Datenbank: Wissens- und Informationsmanagement für die Polizeien des Bundes und der Länder. Polizei Verkehr + Technik (pvt), 71(2), 32–33.

Kötter, K. (1995). 20 Jahre Forschungs- und Entwicklungsstelle für Polizeitechnik (FEStPt). Die Polizei, 86(2/3), 25–28.

Kühnberger, M. (1997). Entwicklungstendenzen im Bereich Führungs- und Einsatzmittel. Polizeitechnisches Institut, Polizei-Führungsakademie.

Kuratorium der Polizei-Führungsakademie (Hrsg.). (1993). Thema heute: Forschung und Entwicklung auf dem Gebiet der Polizeitechnik, (4). Schriftenreihe der Polizei-Führungsakademie. Schmidt-Römhild.

Kuratorium der Polizei-Führungsakademie (Hrsg.). (2000). Aktuelle Problemstellungen im Bereich der Polizeitechnik. Schriftenreihe der Polizei-Führungsakademie, (4). Schmidt-Römhild.

Kuratorium der Polizei-Führungsakademie (Hrsg.). (2002). Polizeitechnik im Wandel. Schriftenreihe der Polizei-Führungsakademie, (3). Sächsisches Druck- und Verlagshaus.

Morgenstern, M., & Honekamp, W. (2024). Identification of technology trends for effective policing. In M. Klein, D. Krupka, C. Winter., M. Gergeleit, L. Martin (Hrsg.), INFORMATIK 2024, Lecture Notes in Informatics (LNI) (S. 391–403), Gesellschaft für Informatik. https://doi.org/10.18420/inf2024_28

OECD. (2023). Technology governance. Organisation for Economic Co-operation and Development. https://www.oecd.org/en/topics/sub-issues/technology-governance.html

PFA. (1998). Jahresbericht 1997. Polizei-Führungsakademie.

PTI. (1998a). Können öffentliche Mobilfunknetze (GSM-Netze) künftig die taktisch-betrieblichen Anforderungen der BOS an ein digitales Funk-Kommunikationssystem erfüllen? Fachtechnische Stellungnahme. Polizei-Führungsakademie.

PTI (Hrsg.). (1998b). Technische Richtlinie BOS: Digitale Fernsehbildübertragung. Polizeitechnisches Institut. Polizei-Führungsakademie.

PTI. (2000). Sind die künftigen öffentlichen UMTS-Mobilfunknetze geeignet, die taktisch-betrieblichen Anforderungen der BOS an ein digitales Funk-Kommunikationssystem zu erfüllen? Fachtechnische Stellungnahme. Polizeitechnisches Institut. Polizei-Führungsakademie.

PTI. (2018). Jahresbericht 2017: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2019). Jahresbericht 2018: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2020). Jahresbericht 2019: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2021). Jahresbericht 2020: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2022). Jahresbericht 2021: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2023). Jahresbericht 2022: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2024). Jahresbericht 2023: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2025). Jahresbericht 2024: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

PTI. (2026). Jahresbericht 2025: Polizeitechnisches Institut (PTI). Deutsche Hochschule der Polizei.

Steffen, W. (1995). Veränderungen in der Polizeilichen Aufgabenwahrnehmung: Gemeinwesenorientierung als moderne Zielperspektive? In H. Schult (Hrsg.), Thema heute: 50 Jahre polizeiliche Bildungsarbeit in Münster-Hiltrup (S. 107–124). Schriftenreihe der Polizei-Führungsakademie.

Schult, H. (1985). 40 Jahre „Hiltrup“: Von der Zentral-Polizeischule zur Polizei-Führungsakademie. Schriftenreihe der Polizei-Führungsakademie.

Verzeichnis der Autorinnen und Autoren

Anosch Amanat, M. Sc., ist Kriminalbeamter im Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz.

EPHK **Andreas Beier**, Magister-, Master-, Diplom-(FH)-Abschluss, Hochschule für Polizei Baden-Württemberg, Fakultät IV: Sozialwissenschaften, war über 19 Jahre im Streifendienst und arbeitete noch mit Fernschreib-Lochstreifen zum Versand „Wichtiger Ereignismeldungen".

Prof. Dr. **Johannes Fähndrich** ist Leiter der Fachgruppe Angewandte Informatik, Cybercrime und Digitale Spuren an der Hochschule für Polizei Baden-Württemberg.

Prof. Dr. **Gundula Gahlen** leitet das Fachgebiet Polizeigeschichte und Politische Bildung an der Deutschen Hochschule der Polizei in Münster.

Prof. Dr. **Wilfried Honekamp** ist Professor für Polizeitechnik mit Schwerpunkt Digitalisierung und Leiter des Polizeitechnischen Instituts der Deutschen Hochschule der Polizei.

Prof. Dr. **Stefan Jarolimek** leitet das Fachgebiet Kommunikationswissenschaft an der Deutschen Hochschule der Polizei in Münster.

Dirk Kunze, M. A., ist beim Landesamt für Zentrale Polizeiliche Dienste der Polizei NRW zuständig für polizeiliche Anwendungen.

Prof. Dr. **Dirk Labudde** ist Leiter der Fach- und Forschungsgruppe Forensic Science Investigation Lab (FoSIL) der Hochschule Mittweida.

KK **Robert Diedrich Ulrich Lippitz**, M. A., wurde für seine Forschung zu Herausforderungen durch Deepfakes für Sicherheitsbehörden auf dem Europäischen Polizeikongress mit dem Zukunftspreis Polizeiarbeit ausgezeichnet. Aktuell befindet er sich auf dem 15. Gemeinsamen Ratanwärterlehrgang von Bundespolizei und BKA.

Prof. a. d. PA Dr. **Andreas Mehlich**, LL. M., ist seit 2019 Professor an der Polizeiakademie Niedersachsen und war zuvor in der niedersächsischen Justiz tätig, zuletzt als Richter am Landgericht.

Prof. a. d. PA Dr. **Roman Povalej** ist seit Juli 2015 an der Polizeiakademie Niedersachsen als Professor für Informations- und Kommunikationstechnik und Cybercrime tätig. Ein besonderes Anliegen ist ihm das Voranbringen der Polizei-Informatik in der Lehre, Forschung und Entwicklung im polizeilichen Kontext.

Prof. **Heiko Rittelmeier** ist Referatsleiter Senior Experts Mobile End-geräte im Geschäftsfeld Digitale Forensik bei der ZITiS und Professor für Allgemeine und Digitale Forensik an der Hochschule Mittweida.

Kilian L. Scholz, MPA, ist Polizeibeamter der Polizeidirektion Hannover, derzeit abgeordnet als Lehrender für Öffentliches Recht an die Polizeiakademie Niedersachsen.

OTL d. R. Dipl.-Kfm. **Lothar H. Schuster** ist seit 1998 in unterschiedlichen Funktionen in der Zulieferindustrie für Polizei und Militär tätig.