Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)863 B

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

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

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

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

privat:
Postfach 580601
D-10415 Berlin

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

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

www.foeps-berlin.org

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

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

Per E-Mail an: innenausschuss@bundestag.de

Datum: 05. Juni 2021

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

Sehr geehrte Damen und Herren,

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

1. Digitalisierung im Kontext polizeilicher Techniknutzung

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

1.1 Entwicklungsdynamik der polizeilichen Techniknutzung seit den 1970erJahren

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

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

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

1.2 Digitalisierung von Arbeitsabläufen und von Datenverarbeitungsvorgängen: Grundrechtliche Dimensionen einbeziehen

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

---

1 Näher zu diesem Strukturproblem Aden 2019.

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

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

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

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

2. Chancen und Risiken der Digitalisierung einbeziehen

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

2.1 Akzeptanz der Betroffenen durch Transparenz fördern

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

---

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

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

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

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

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

---

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

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

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

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

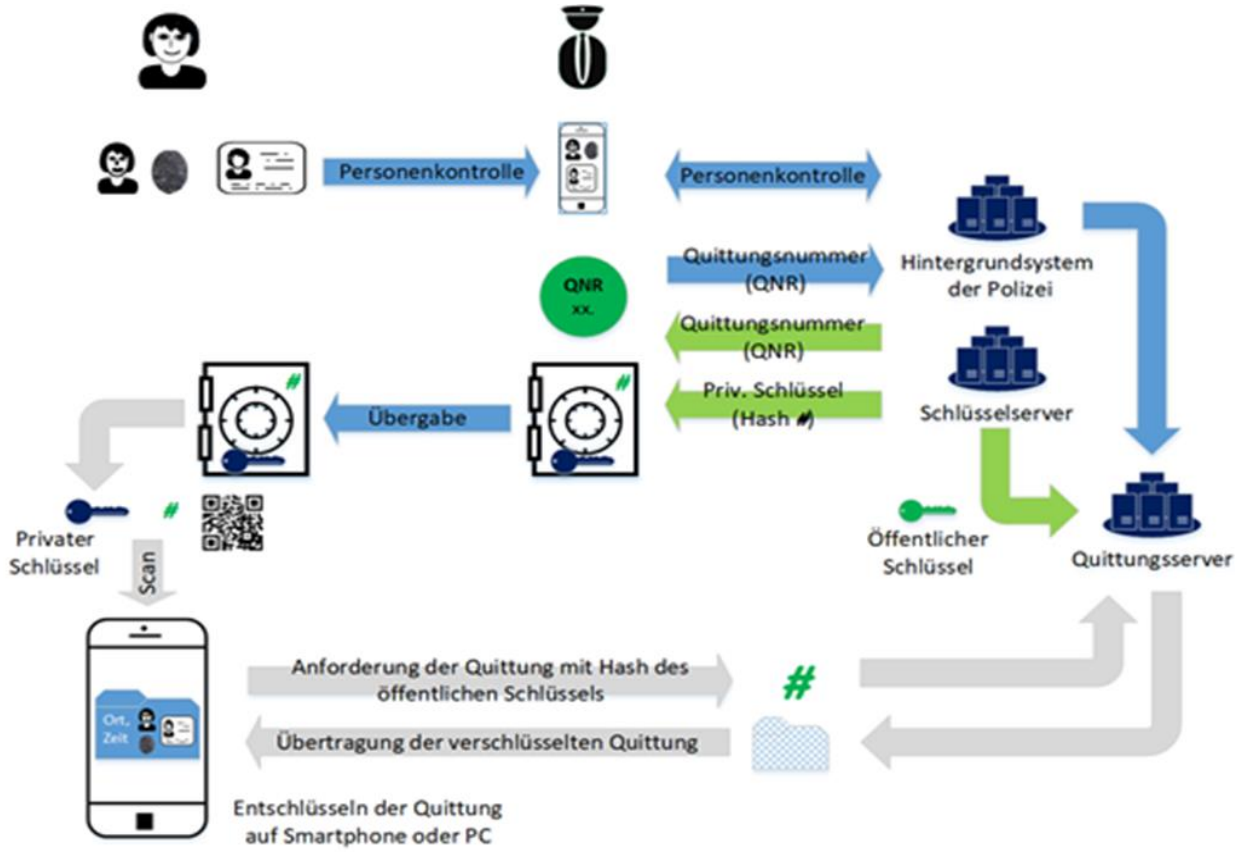

Abbildung 1: Ablauf der Quittungserstellung (Bildquelle: MEDIAN-Projekt/ Bundesdruckerei/Uwe Rabeler)

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

2.2 Missbrauchsrisiken vorbeugen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Gez. Prof. Dr. Hartmut Aden

Literatur

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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