Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung

Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie

Hartmut Aden, *Hochschule für Wirtschaft und Recht, Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin), Alt-Friedrichsfelde 60, 10315 Berlin (Hartmut.Aden@hwr-berlin.de)* *https://orcid.org/0000-0001-8997-6867*
Jan Fährmann, *Hochschule für Wirtschaft und Recht, FÖPS Berlin (Jan.Faehrmann@hwr-berlin.de)* *https://orcid.org/0000-0003-4356-1150*

Seit 2018 ist auch für Datenverarbeitungsvorgänge der Polizei nach dem EU-Datenschutzrecht bei hohen Risiken für die Rechte und Freiheiten der Betroffenen eine Datenschutz-Folgenabschätzung (DSFA) vorgeschrieben. Dieser Beitrag untersucht die Möglichkeiten, die diese verbindliche DSFA für eine transparente, grundrechtsschonende und demokratisch kontrollierbare Polizeiarbeit bietet. Er zeigt, dass sich viele Akteure der Innenpolitik und Polizei mit Transparenz schwertun, sodass eine demokratische Kontrolle, die grundrechtsschonendes Polizeihandeln sicherstellen soll, nur eingeschränkt funktioniert. Dem kann durch höhere Transparenzstandards bei der polizeilichen Datenverarbeitung sowie durch eine grundrechtsschonende Technikgestaltung nach dem Grundsatz ***Privacy by Design*** entgegengewirkt werden.

Data protection assessment and transparency deficits in technology use
An analysis using the example of police data processing

Since 2018, EU data protection law requires a Data Protection Impact Assessment (DPIA) for any data processing that involves high risks to the rights and freedoms of natural persons. This paper examines the possibilities for transparent and fundamental rights-protecting policing that this legal framework offers. Many politicians and police officials tend to place more emphasis on security than on transparency, democratic accountability of policing, and high standards of privacy. This can be counteracted by higher transparency standards in police data processing and by designing technology based on privacy by design.

Keywords: *data protection, policing, privacy, technology, accountability*

https://doi.org/10.14512/tatup.29.3.24
Submitted: 24. 05. 2020. Peer reviewed. Accepted: 21. 10. 2020

Immer mehr prägen „smarte“ Geräte den Alltag. Die darin enthaltenen technischen Anwendungen werden zunehmend vernetzt und tauschen permanent Daten aus. Dementsprechend steigt auch das polizeiliche Interesse an Datenverarbeitungstechnologien (Fährmann 2020, S. 228). Polizeilicher Technikeinsatz führt oft zu intensiveren Grundrechtseingriffen, wobei insbesondere die Telekommunikationsfreiheit und das Allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme betroffen sind (Fährmann et al. 2020). Neue technische Möglichkeiten können zudem erheblichen Einfluss auf gesellschaftliche Verhältnisse und Machtstrukturen haben (Roßnagel 2020; Grunwald 2010 b, S. 29), z. B. indem sie einseitig Zugang zu Informationen eröffnen. Sie können sich auch auf demokratische Herrschaftsstrukturen auswirken, etwa wenn ihre Ausgestaltung demokratische Kontrolle erschwert (Narr 2003; Grunwald 2010 b, S. 27). Technische (Überwachungs-)Maßnahmen können einen Einschüchterungseffekt entfalten, wodurch demokratische Partizipationsmöglichkeiten beeinträchtigt werden, z. B. die Wahrnehmung der Versammlungs- und Meinungsfreiheit. Wie sich Technik auf Machtverhältnisse auswirkt, hängt von ihrer konkreten Ausgestaltung ab. So kann Technik auch Freiheiten zur Grundrechtsausübung erweiterten und eine bessere Kontrolle ermöglichen, z. B. durch die Steigerung von Transparenz behördlicher Abläufe (von Lucke 2010; Roßnagel 2020, S. 224).

Dieser Beitrag geht von der Hypothese aus, dass Entwicklung und Nutzung polizeilicher Datenverarbeitungstechnologien – wie etwa international vernetze Datenbanken aber auch Mittel zur Datenerhebung wie Kameras – für die Betroffenen zumeist weitgehend intransparent sind. Die hohe Geschwindigkeit der Technikentwicklung verstärkt solche Transparenzdefizite (vgl. Grunwald 2010 b, S. 49). Nicht nur für die Bevölkerung,

sondern auch für gesetzgebende Parlamentarier*innen und gesetzesanwenden Gerichte ist nur begrenzt nachvollziehbar, wie polizeiliche Technik genau funktioniert und wie sie sich auf den Grundrechtsgebrauch auswirkt. Damit sind Transparenzdefizite polizeilicher Datenverarbeitung auch Teil eines Demokratiedefizits. Demokratische Entscheidungen können gegenüber dem repräsentierten Volk nur auf der Basis ausreichender Informationen verantwortet werden (Velten 1996, S. 15). Transparenz stellt damit ein konstitutives Element demokratischer Entscheidungen dar (Riese 2019, S. 114; Stehr und Wallner 2010, S. 12).

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.

Dieser Beitrag betrachtet die Ursachen und Folgen von (In-) Transparenz polizeilicher Datenverarbeitung aus einer interdisziplinären rechts- und politikwissenschaftlichen Perspektive. Zunächst werden Transparenzdefizite der polizeilichen Techniknutzung betrachtet. Auf dieser Basis wird untersucht, welchen Beitrag die DSFA für die Herstellung von Transparenz des polizeilichen Technikeinsatzes leisten kann. Dabei geht der Beitrag auch der Frage nach, inwieweit die DSFA eine neue Variante der Technikfolgenabschätzung (TA) ist.

Transparenzdefizite polizeilicher IT-Anwendungen

Gesetzliche Regelungen werden oft schon nach kurzer Zeit obsolet, weil neue technische Entwicklungen schwerwiegendere Eingriffsmaßnahmen ermöglichen als zuvor. Die Gesetzgebung tendiert daher zur Schaffung allgemein gehaltener, weitgehend unbestimmter Eingriffsbefugnisse (Aden und Fährmann 2019 a, 2019 b). Diese Tendenz zur Unbestimmtheit von Eingriffsnormen wird noch dadurch verstärkt, dass polizeiliche Eingriffsbefugnisse zunehmend nicht mehr an konkrete Gefahren und Straftaten anknüpfen, sondern Eingriffe bereits in deren Vorfeld legitimieren, z. B. wenn die Polizei bei der Vorbereitung von Einsatzschwerpunkten auf Daten aus dem *predictive policing* zurückgreift, bei dem aus Kriminalitätsdaten zukünftige Risiken vorausberechnet werden (Thurn und Egbert 2019, S. 73 f.). Durch den Trend zur Analyse großer Datenbestände *(Big Data),* auch mit Unterstützung künstlicher Intelligenz, dürfte sich die polizeiliche Tätigkeit in Zukunft sogar noch weiter in das Vorfeld von Gefahren und Straftaten verlagern.

Weitgehend ungeregelt und damit intransparent ist 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 (Fährmann et al. 2020). Unbestimmte Eingriffsbefugnisse führen dazu, dass (potenziell) Betroffene nicht ohne Weiteres nachvollziehen können, was genau die Polizei darf. Befugnisse zur verdeckten Datenerhebung, z. B. für Online-Durchsuchungen, im Rahmen verdeckter Observationen oder durch verdeckte Ermittler*innen, verstärken den Trend zu intransparenter polizeilicher Datenerhebung (Velten 1996, S. 15; Albers und Weinzierl 2010).

Unbestimmte Eingriffsbefugnisse führen dazu, dass Betroffene nicht ohne Weiteres nachvollziehen können, was genau die Polizei darf.

Aufgrund dieser Intransparenz ist die polizeiliche Datenverarbeitung nur selten Gegenstand gerichtlicher Kontrolle, zumal die Betroffenen auch nicht über jede Datenverarbeitung informiert werden. Selbst bei offener Datenerhebung, also in Fällen, in denen Daten wie bei einer Ausweiskontrolle so erhoben werden, dass die Erhebung für die Betroffenen erkennbar ist, können diese kaum nachvollziehen, wie ihre Daten in den polizeilichen Systemen verarbeitet werden. Weitgehend intransparent ist z. B. der Datenabgleich, obwohl er oft offen abläuft, mit dem im alltäglichen Polizeidienst geprüft wird, ob zu einer Person Informationen in den polizeilichen Systemen vorliegen. Betroffene können dadurch verunsichert werden, dass für sie in der Regel nicht ersichtlich ist, mit welchen Datenbanken ihre Daten abgeglichen werden, ob ihre Daten gespeichert werden und welche langfristigen Konsequenzen der Abgleich für sie hat (Aden et al. 2020, S. 98 f.). Auch, wenn es rechtlich legitim sein kann, gewisse Informationen mit polizeilichen Datenbanken abzugleichen und diese ggf. auch zurückzuhalten, z. B. zur Eigensicherung der Polizist*innen beim Umgang mit Menschen, die als gewaltbereit bekannt sind, könnten Polizist*innen Betroffenen sehr wohl die Gründe der Kontrolle sowie den abstrakten Ablauf des Datenabgleichs erklären und so Transparenz schaffen,

soweit die Einsatzsituation dies zulässt. Allerdings gibt es kaum gesetzliche Vorgaben, die ein transparentes Verfahren eindeutig vorschreiben oder wirkungsvolle und systematische Transparenzmechanismen etablieren. Aus den Verwaltungsverfahrensgesetzen folgen Pflichten zur Begründung von Verwaltungsakten nur, wenn diese schriftlich ergehen (§ 39 VwVfG), was bei polizeilichen Einsätzen im öffentlichen Raum die Ausnahme ist. Unter Heranziehung von verfassungsrechtlichen Transparenzvorgaben (z. B. BVerfGE 40, 296 (327), Entscheidungen des Bundesverfassungsgerichts) bestehen gleichwohl Aufklärungspflichten, die bisher allerdings nur in wenigen Landesgesetzen und nur bezüglich einzelner Maßnahmen konkretisiert wurden. Ob und ggf. wie intensiv polizeiliche Maßnahmen den Betroffenen erläutert werden, ist bei alltäglichen Einsätzen im öffentlichen Raum daher zumeist den handelnden Beamt*innen überlassen. Die ohnehin aufgrund des staatlichen Gewaltmonopols bestehende überlegende Stellung von Polizist*innen bei Interaktionen mit Bürger*innen wird so erheblich verstärkt. Dies kann im schlimmsten Falle dazu führen, dass Menschen Orte oder Veranstaltungen meiden, wenn sie mit einer Datenverarbeitung rechnen (Aden et al. 2020, S. 94).

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 (Grunwald 2010 a, S. 85; Fährmann et al. 2020, S. 144).

Im Ergebnis bestehen somit strukturelle Risiken von Intransparenz gegenüber den vom Technikeinsatz Betroffenen, den Parlamenten und anderen staatlichen Kontrollinstanzen.

Polizeiliche Datenschutz-Folgenabschätzung

Der Ausbau der polizeilichen Informationstechnik kann zu beträchtlichen Risiken für die Privatsphäre der Menschen führen. Aufgrund des großen Umfangs vorhandener Datenbestände und automatisierter Auswertungsmöglichkeiten sind aus polizeilichen Datenbeständen Rückschlüsse auf Personen und ihr Verhalten generierbar, was ein umfassendes *Profiling* möglich machen kann (Fährmann 2020). Datenbestände werden zunehmend miteinander vernetzt, etwa die Polizei- und Migrationsdatenbanken der Europäischen Union (zur Kritik: Aden 2020).

Daher hat die Bewertung der Datenschutzqualität bei Auswahlentscheidungen für die Einführung neuer Technologien an Bedeutung gewonnen. Folgerichtig ist die DSFA nun vorgeschrieben, wenn eine Datenverarbeitung, „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat (§ 67 Abs. 1 BDSG, Bundesdatenschutzgesetz). Dabei ist auch die Technologiegestaltung zu bewerten (Fährmann et al. 2020, S. 144 f.). Sie ist ein weiteres rechtsverbindliches Instrument zur Abschätzung von Auswirkungen der Technik (Gola et al. 2019, § 67 Rn. 7), welches in bestimmten Fällen auch gerichtlich eingeklagt werden kann (Nolde 2018, C III, Rn. 1 ff.).

TA und DSFA sind jeweils systematische, prozedurale Instrumente, um frühzeitig die Möglichkeiten, Folgen und Nebenwirkungen von technischen Entwicklungen zu evaluieren, um Risiken rechtzeitig zu erkennen und einmal eingeführte Technik optimal nutzen zu können (Friedewald 2017, S. 67; Decker 2007, S. 29 ff.). Die DSFA soll einer missbräuchlichen Datenmacht, z. B. von großen Konzernen und Sicherheitsbehörden, entgegenwirken (Friedewald 2017, S. 66). Technik muss so gestaltet werden, dass sie Grundrechte schützt und demokratische Teilhabemöglichkeiten eröffnet (Roßnagel 2020, S. 222 ff.). Dazu muss der gesamte Datenverarbeitungsvorgang systematisch mit Blick auf datenschutzrechtliche Risiken begutachtet werden. Risikominimierende Maßnahmen sind zu ergreifen und zu dokumentieren (Wichtermann 2016, S. 797; Friedewald 2017, S. 67). Die DSFA ist damit eine spezielle Form der TA.

Unzulängliche Vorgaben für die polizeiliche Datenschutz-Folgenabschätzung

Wie eine DSFA in der polizeibehördlichen Praxis abläuft, ist empirisch bisher weitgehend unerforscht. Ausgangspunkt der Überlegungen ist deshalb hier der normative Rahmen, wie er 2016 durch das EU-Datenschutzrecht etabliert wurde. Für die Polizei kann sowohl § 35 DSGVO als auch § 67 BDSG einschlägig sein, letzterer wenn ein Bezug zu Straftaten besteht, was vielfach der Fall sein wird. Für die Landespolizeien können die Datenschutz- und Polizeigesetze der Länder konkretisierende Regelungen enthalten. Die DSFA wird von den Verantwortlichen, also hier der Polizei, selbst durchgeführt. Eine Beteiligung der zuständigen Landes-Datenschutzbeauftragten oder externer Expert*innen ist möglich, aber nicht vorgeschrieben. Andere Akteure sind nicht zwingend zu beteiligen, anders als nach Art. 35 Abs. 9 DSGVO, wo eine Beteiligungsmöglichkeit der Betroffenen vorgesehen ist. Bezüglich des Verfahrens gibt es keine klaren gesetzlichen Vorgaben. Die Regelungen in § 67 Abs. 4 BDSG sind sehr allgemein gehalten; sie beziehen sich abstrakt auf die Verhältnismäßigkeit der Datenverarbeitung und Maßnahmen zum Umgang mit Gefahren für die Betroffenen.

Zunächst ist festzuhalten, dass bei der Einführung neuer datenverarbeitender Geräte und Verfahren zur Gefahrenabwehr und Strafverfolgung im Regelfall ein hohes Risiko für die Privatsphäre Betroffener besteht, so dass eine DSFA erforderlich ist (Borell und Schindler 2019, S. 394 f.). Dies folgt bereits daraus, dass ein Großteil der personenbezogenen Daten, die für die Polizeiarbeit von Interesse sind, hoch sensible Informationen enthalten, z. B. bezüglich des Verdachts, Straftaten begangen zu haben.

Die DSFA richtet sich nach normativen Kriterien, die aus den Grund- und Menschenrechten und aus den spezielleren Anfor-

derungen der DSGVO und der Datenschutzgesetze folgen. Insofern handelt es sich nicht um eine gänzlich ergebnisoffene TA, sondern um ein rechtlich formalisiertes Verfahren, welches nur datenschutzrechtliche Risiken im Blick hat, obwohl Polizeitechnik auch andere Risiken erzeugen kann, etwa Verletzungsrisiken durch Waffen.

Die polizeiliche DSFA stößt allerdings auf die Schwierigkeit, dass viele Akteure in Innenpolitik und Polizei anscheinend in erster Linie daran interessiert sind, möglichst viele Daten zu verarbeiten, weniger an einer wirksamen Begrenzung und an qualitativ akkuraten Daten (zur Kritik: Aden und Fährmann 2018, S. 19 ff.). Dabei zielte die Einführung der DSFA gerade darauf, die Datenverarbeitung sowohl effizienter zu gestalten als auch Grundrechtseingriffe möglichst gering zu halten (vgl. Peissl 2012, S. 144 f.). Zu viele Informationen können dazu führen, dass die polizeiliche Arbeit ineffizient und ineffektiv wird, da die Polizei die Qualitätssicherung für so große Datenmengen kaum bewältigen kann (Fährmann 2020, S. 231; Aden 2020, S. 104 f.) und daher möglicherweise relevante Daten übersieht oder aufgrund fehlerhafter Daten agiert.

Bei der Einführung neuer datenverarbeitender Verfahren zur Strafverfolgung besteht im Regelfall ein hohes Risiko für die Privatsphäre Betroffener.

Weil Polizeibehörden in der Regel möglichst viele Daten verarbeiten möchten, sind die Interessen hier anders gelagert als z. B. bei der Umweltverträglichkeitsprüfung, bei der Umweltschutzbelange mit der Verhältnismäßigkeit der Kosten abgewogen werden müssen, die Umweltschutzauflagen für Investoren nach sich ziehen. Zusätzliche technische Eingriffsbefugnisse können die alltägliche Arbeit aus der polizeilichen Perspektive (vermeintlich) deutlich angenehmer und effektiver gestalten. Ein Verzicht auf Transparenz vermeidet zudem lästige Diskussionen mit Betroffenen und der (Fach-)Öffentlichkeit. Auch Dokumentationspflichten sind für Praktiker*innen mit zusätzlichem Aufwand verbunden und können daher als störend empfunden werden. Ferner birgt weniger Kontrolle ein geringeres Sanktionsrisiko für Fehlverhalten, welches neben dienstrechtlichen auch strafrechtliche Konsequenzen haben kann. Insofern ist es kritisch zu sehen, wenn die Polizei der wesentliche Akteur der DSFA ist, da so eine einseitige Herangehensweise zu befürchten ist. Die Umsetzung der EU-Vorgaben sollte in der deutschen Gesetzgebung nachgebessert werden.

Transparenz polizeilicher Datenschutz-Folgenabschätzung und partizipative Ansätze

Aufgrund der komplexen Entscheidungsprozesse über neue Technologien unterliegt deren Bewertung hohen Transparenzanforderungen (Grunwald 2010c, S. 317 f.). Eine angemessene Balance zwischen Sicherheitsbelangen und effektivem Grundrechtsschutz erfordert, dass alle Perspektiven berücksichtigt werden. Daher wird bei der TA eine partizipative Ausrichtung als unverzichtbar eingeschätzt. Die Perspektive der Betroffenen ist essentiell, um die tatsächlichen Auswirkungen der Verarbeitung bestimmen zu können. So kann auch Akzeptanz für neue Technologien geschaffen werden (Abels und Bora 2013, S. 113 ff.), die allerdings von der Art der Beteiligung, den tatsächlichen Einflussmöglichkeiten und den Interessen der beteiligten Akteure abhängt (Petermann und Scherz 2005, S. 51). Jedenfalls wird der Prozess durch Transparenz und Partizipation demokratischer (Renn 1993, S. 80). Ohne Transparenz kann von der Öffentlichkeit hingegen noch nicht einmal eingeschätzt werden, ob eine DSFA überhaupt durchgeführt wurde oder ob diese sachgerecht war.

Die Komplexität der zunehmend international vernetzten polizeilichen Datenverarbeitung spricht für eine unabhängige DSFA unter Einbeziehung spezialisierter Expert*innen und Nichtregierungsorganisationen. Wie generell bei der TA sind der Entwicklungsstand der Technik, die beteiligten Akteure sowie deren Interessen, der institutionelle Kontext und die bestehenden Gestaltungsspielräume in die Betrachtung einzubeziehen (vgl. Grunwald 2010b, S. 37). Gerade bei der polizeilichen Datenverarbeitung kann die Perspektive der vom Technikeinsatz Betroffenen sich grundlegend von den Perspektiven und Interessen der Technikanwender*innen unterscheiden, da es hier oft um die Balance zwischen dem Interesse an möglichst vielen Informationen und dem Grundrechtsschutz geht. In eine partizipative DSFA aus der Betroffenenperspektive könnten auch Interessenvertreter*innen derjenigen Menschen einbezogen werden, die überdurchschnittlich oft von polizeilichen Maßnahmen betroffen sind, z. B. aufgrund ihres Aussehens oder ihrer politischen Betätigung.

Die Einbindung der internen Datenschutzbeauftragten, die eine institutionelle Nähe zu der jeweiligen Behörde aufweisen, reicht nach der hier vertretenen Auffassung nicht, da diese in der Regel nicht hinreichend unabhängig sind. Auch beschränkt sich die Rolle der Datenschutzbeauftragten bei der polizeilichen DSFA auf eine Beteiligung; ein Veto oder andere weitergehende Interventionsrechte sind bisher nicht gesetzlich vorgesehen. Damit fehlt eine effektive externe Beteiligung gerade im polizeilichen Bereich, der durch besonders weitreiche Informationseingriffe geprägt ist. In der deutschen Umsetzung der EU-Vorgaben ist auch nicht geregelt, wer neben der Polizei Zugang zu den Ergebnissen hat.

Das verfassungsrechtliche Transparenzgebot und das Gebot effektiver Umsetzung des EU-Rechts erfordern somit eine ausweitende Auslegung dieser restriktiven Richtlinienumsetzung. Zumindest das Ergebnis der DSFA muss in einer Form veröffentlicht werden, die eine informierte Debatte ermöglicht. Wie detailliert die Veröffentlichung sein muss, hängt u. a. von der Tragweite eventueller Geheimhaltungsinteressen ab. Gänzlich vorenthalten werden kann eine polizeiliche DSFA der Bevölkerung nicht, zumindest an den abstrakten technischen Abläufen wird im Regelfall kein legitimes Geheimhaltungsinteresse bestehen.

Technische Transparenzmechanismen

Die DSFA sollte nicht nur transparent und partizipativ ablaufen, sondern hat zu betrachten, wie datenschutzrechtliche Risiken minimiert und wie Transparenz während der Datenverarbeitung hergestellt werden kann, um unverhältnismäßige Grundrechtseingriffe und Abschreckungseffekte zu vermeiden.

Der Grundsatz *Privacy by Design* ist ein Schlüsselkonzept zur Verbesserung von Datenschutzstandards und zur Herstellung von Transparenz an der Schnittstelle zwischen Technik und Recht, das auch bei der DSFA eine zentrale Rolle spielt. Dieser Grundsatz besagt, dass die datenschutzkonforme Technikutzung 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 (Čas 2010, S. 260 f.). Videoaufnahmen können z. B. ganz oder teilweise verpixelt, gespeicherte Daten einem automatisierten Löschkonzept unterworfen, Datenverarbeitungssysteme mit technisch mehrfach gesicherten Zugangssystemen versehen werden. Das Datenschutzrecht und die DSFA sollen nicht nur negative Technikfolgen verringern, sondern bereits während der Technikentwicklung sicherstellen, dass Grundrechtseingriffe so milde und transparent wie möglich sind, etwa durch zwingende Voreinstellungen im Benutzungsmenü polizeilicher Geräte. Mobile Geräte können z. B. so ausgestaltet werden, dass ein Zugriff auf Eingriffsmaßnahmen nur dann möglich ist, wenn die jeweiligen Tatbestandsvoraussetzungen erfüllt sind (Aden et al. 2020, S. 98 ff.; Fährmann et al. 2020, S. 145).

Transparenz kann auch durch zu veröffentlichende statistische Auswertungen gefördert werden, indem Verarbeitungsvorgänge ohne Personen- oder Einsatzbezug dokumentiert werden, etwa wie oft Informationseingriffe genutzt wurden und welche Konsequenzen sie hatten. Auch könnten die Betroffenen technisch generierte Nachweise über die Datenverarbeitung erhalten, z. B. über *Quick Response (QR) Codes,* die den Zugang zu weiteren netzbasierten Informationen über die Praxis der Datenverarbeitung und ihre rechtlichen Begrenzungen eröffnen. Die Polizei sollte ihre Datenverarbeitungspraxis öffentlich gut nachvollziehbar erläutern, etwa auf ihrer Webseite, und damit zugleich die Anforderungen des § 55 BDSG erfüllen. Allerdings kann technikbasierte Transparenz die nachvollziehbare Ausgestaltung von Eingriffsmaßnahmen durch Polizist*innen nicht vollständig ersetzen. Professionelle Kommunikation bleibt trotz Digitalisierung eine wesentliche transparenz- und vertrauensbildende Komponente der polizeilichen Arbeit.

Fazit

Dieser Beitrag hat gezeigt, dass die Datenschutz-Folgenabschätzung in Deutschland für den polizeilichen Bereich bislang nur unzulänglich ausgestaltet wurde, ebenso die auf der Richtlinie (EU) 2016/680 basierenden Gesetze.

Die DSFA als rechtlich strukturierte Variante der Technikfolgenabschätzung bietet Chancen, die Nutzung von Informationstechnik durch die Polizei datenschutzfreundlich, grundrechtsschonend, und transparent auszugestalten. Eine solche Transparenz kann nicht nur die Akzeptanz polizeilicher Maßnahmen steigern. Sie kann auch aggregierte Daten produzieren, die Parlamente und (Fach-)Öffentlichkeit nutzen können, wenn sie demokratische Kontrolle über die Polizei als Organ des staatlichen Gewaltmonopols mit weitreichenden Befugnissen ausüben. Allerdings hat der Beitrag auch gezeigt, dass sich die Bereitschaft zur Herstellung von Transparenz im Rahmen der DSFA in Innenpolitik und Polizeipraxis häufig in Grenzen hält. Daher bleibt abzuwarten, inwieweit die EU Deutschland zu Nachbesserungen im Interesse einer effektiven Umsetzung des EU-Datenschutzrechts und des Grundrechtsschutzes für die Bürger*innen zwingt.

Die Polizei sollte ihre Datenverarbeitungspraxis öffentlich gut nachvollziehbar erläutern.

Literatur

Abels, Gabriele; Bora, Alfons (2013): Partizipative Technikfolgenabschätzung und -bewertung. In: Georg Simonis (Hg.): Konzepte und Verfahren der Technikfolgenabschätzung. Wiesbaden: Springer, S. 109–128. DOI: 10.1007/978-3-658-02035-4_7.

Aden, Hartmut (2020): Interoperability between EU policing and migration databases. Risks for privacy. In: European Public Law 26 (1), S. 93–108.

Aden, Hartmut; Bosch, Alexander; Fährmann, Jan (2020): Kontrollieren – aber wie? Können technische Innovationen die Akzeptanz für polizeiliche Personenkontrollen verbessern? In: Hermann Groß und Peter Schmidt (Hg.): Polizei und Migration. Empirische Polizeiforschung XXIII. Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 90–108.

Aden, Hartmut; Fährmann, Jan (2018): Polizeirecht vereinheitlichen? Kriterien für Muster- Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive. Berlin. Online verfügbar unter https://www.boell.de/de/2018/12/12/polizeirecht-vereinheitlichen, zuletzt geprüft am 02. 10. 2020.

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

Aden, Hartmut; Fährmann, Jan (2019 b): Wie lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen? In: Vorgänge Nr. 227, 58 (3), S. 95–106.

Albers, Marion; Weinzierl, Ruth (2010): Wandel der Sicherheitspolitik. Menschenrechtsorientierte Evaluierung als Kontrollinstrument. In: Marion Albers und Ruth Weinzierl (Hg.): Menschenrechtliche Standards in der Sicherheitspolitik. Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen. Baden-Baden: Nomos, S. 9–12. DOI: 10.5771/9783845221939-9.

Borell, Anne; Schindler, Stephan (2019): Polizei und Datenschutz. Vorgaben der neuen JI-RL für technische und organisatorische Maßnahmen zur Gewährleistung datenschutzkonformer polizeilicher Datenverarbeitung. In: Klaus David, Kurt Geihs, Martin Lange und Gerd Stumme (Hg.): Informatik 2019. 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft. Bonn: Gesellschaft für Informatik e. V. (GI), S. 393–406.

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, S. 257–262. DOI: 10.1007/978-90-481-8865-9_15.

Decker, Michael (2007): Praxis und Theorie der Technikfolgenabschätzung. Erste Überlegungen zu einer methodischen Rekonstruktion. In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 16 (1), S. 25–34. DOI: 10.14512/tatup.16.1.25.

Fährmann, Jan (2020): Digitale Beweismittel und Datenmengen im Strafprozess. In: MMR – Multimedia und Recht 23 (4), S. 228–233.

Fährmann, Jan; Aden, Hartmut; Bosch, Alexander (2020): Technologieentwicklung und Polizei. Intensivere Grundrechtseingriffe auch ohne Gesetzesänderung. In: Kriminologisches Journal 52 (2), S. 135–148.

Friedewald, Michael (2017): Datenschutz-Folgenabschätzung. In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 26 (1–2), S. 66–71. DOI: 10.14512/tatup.26.1-2.66.

Gola, Peter et al. (2019): BDSG. Bundesdatenschutzgesetz. München: C. H. Beck.

Grunwald, Armin (2010 a): 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, S. 85–92. DOI: 10.5771/9783845271132-85.

Grunwald, Armin (2010 b): Technikfolgenabschätzung. Eine Einführung. Berlin: edition sigma. DOI: 10.5771/9783845271057.

Grunwald, Armin (2010 c): Transparenz in der Technikfolgenabschätzung. Konzeptionelle Erwartungen und ihre Einlösung. In: Stephan Jansen, Eckhard Schröter, Nico Stehr und Cornelia Wallner (Hg.): Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 309–347. DOI: 10.1007/978-3-531-92466-3_21.

Von Lucke, Jörn (2010): Transparenz 2.0. Transparenz durch E-Government. In: Stephan Jansen, Eckhard Schröter, Nico Stehr und Cornelia Wallner (Hg.): Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 396–412. DOI: 10.1007/978-3-531-92466-3_25.

Narr, Wolf-Dieter (2003): Die Technologisierung der Polizei. Eine Einleitung. In: CILIP Nr. 76 (3), S. 6–11.

Nolde, Malaika (2018): Dokumentationspflichten im Unternehmen. III. Datenschutz-Folgenabschätzung und Konsultation. In: Ansgar Koreng und Bilal Abedin (Hg.): Formularhandbuch Datenschutzrecht. München: C. H. Beck.

Petermann, Thomas; Scherz, Constanze (2005): TA und (Technik-)Akzeptanz (forschung). In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 14 (3), S. 45–53. DOI: 10.14512/tatup.14.3.45.

Peissl, Walter (2012): Datenschutz als Designmerkmal. In: Michael Decker, Armin Grunwald und Martin Knapp (Hg.): Der Systemblick auf Innovation. Technikfolgenabschätzung in der Technikgestaltung. Berlin: edition sigma, S. 141–172.

Renn, Ortwin (1993): Technik und gesellschaftliche Akzeptanz. Herausforderungen der Technikfolgenabschätzung. In: GAIA, 2 (2), S. 67–83.

Riese, Dorothee (2019): Grenzen der Transparenz. Geheimhaltung in demokratischen Systemen. In: Vincent August und Fran Osrecki (Hg.): Der Transparenzimperativ. Normen-Praktiken-Strukturen. Wiesbaden: Springer VS, S. 95–122. DOI: 10.1007/978-3-658-22294-9_4.

Roßnagel, Alexander (2020): Technik, Recht und Macht. Aufgabe des Freiheitsschutzes in Rechtsetzung und -anwendung im Technikrecht. In: MMR – Multimedia und Recht 23 (4), S. 222–228.

Stehr, Nico; Wallner, Cornelia (2010): Transparenz. Einleitung. In: Stephan Jansen, Eckhard Schröter, Nico Stehr und Cornelia Wallner (Hg.): Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 9–19. DOI: 10.1007/978-3-531-92466-3_1.

Thurn, Roman; Egbert, Simon (2019) Predictive Policing. Die Algorithmisierung der Polizei als Risiko für die Bürgerrechte. In: Vorgänge Nr. 227, 58 (3), S. 71–84.

Velten, Petra (1996): Transparenz staatlichen Handelns und Demokratie. Zur Zulässigkeit verdeckter Polizeitätigkeit. Pfaffenweiler: Centaurus-Verlag.

Wichtermann, Marco (2016): Die Datenschutz-Folgenabschätzung in der DS-GVO. Die Folgenabschätzung als Nachfolger der Vorabkontrolle. In: Datenschutz und Datensicherheit (DuD) 39 (12), S. 797–801.

PROF. DR. HARTMUT ADEN
ist Jurist und Politikwissenschaftler, seit 2009 Professor an der Hochschule für Wirtschaft und Recht Berlin, seit 2016 mit einer Professur für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft und Gründungsmitglied des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS Berlin, seit 2013).

DR. JAN FÄHRMANN
ist Jurist und Kriminologe und arbeitet seit 2018 als wissenschaftlicher Mitarbeiter im Forschungsinstituts für Öffentliche und Private Sicherheit. Vorher hat er in der Strafverteidigung gearbeitet und zu einem juristisch/kriminologischen Thema promoviert.