

## Kapitel V. Zukünfte der Polizei: Zwischen einer Polizei der Zukünfte und einer Zukunft ohne Polizei

Wie sich im Rahmen der bisherigen Untersuchung gezeigt hat, ist die Polizei als zentrale Akteurin der formellen Sozialkontrolle aufs Engste mit dem informationstechnologischen Wandel verwoben. Der Grad und die Weise ihrer organisationalen und technischen Adaption an die Dynamiken und Logiken des Massendatenparadigmas wird maßgeblich mit über ihre weitere Entwicklung als Institution bestimmen. Damit wird ihr technologischer Entwicklungsgrad von zentralem Einfluss darauf sein, welche Rolle die Polizei in Deutschland im gesamtgesellschaftlichen Gefüge einnehmen wird und inwiefern sie in diesem Kontext soziale Kontrolle ausüben kann.

Dabei sind der Modus der Produktion sozialer Ordnung und die Ausübung sozialer Kontrolle in einer Gesellschaft keine schlichten Funktionen technologischer Möglichkeiten, sie sind, mit anderen Worten, nicht technologisch determiniert. So ist Massenüberwachung keinesfalls das „natürliche“ oder zwangsläufige Ergebnis der gesellschaftlichen Massendatenproduktion und -verarbeitung, sondern eine Entwicklung die durch – intentionale wie nicht-intentionale – menschliche Handlungen und Entscheidungen aus den unterschiedlichen gesellschaftlichen Feldern beeinflusst wird, die mit dem Massendatenphänomen verschränkt sind. Getragen werden diese Aktivitäten immer von wertegeleiteten Annahmen, wie man etwa an der zutiefst normativen Natur der Verknüpfung von Risikozuschreibungen mit massendatenbasierten Korrelationen ablesen kann. So heißt es bei *Završnik* zutreffend: „[A]scribing weight to past correlations in the form of oscillating between the past and present is an inherently political/value-based process.“<sup>2154</sup> Aber nicht nur die Zuschreibung von Risiken wird im sicherheitspolitischen Diskurs unter dem Eindruck verschiedener Prämissen, Zielvorstellungen oder Zweckmäßigkeitserwägungen verhandelt. Vielmehr steht das ganze polizeiliche Informationswesen mit seinen unterschiedlichen technischen Ausprägungen in einer diskursiven Sphäre, in der Wechselwirkungen zwischen den spezifischen sozialen, kulturellen, politischen und wirtschaftlichen Zwängen einer Gesellschaft darüber entscheiden, ob

---

2154 *Završnik* in *Završnik* (Hrsg.), *Big Data, Crime, and Social Control*, 3 (13).

und inwiefern bestimmte Technologien sich im gesellschaftlichen Geflecht entfalten können.<sup>2155</sup> Soll es umfassende biometrische Gesichtserkennung zu Fahndungszwecken oder intelligente Videoüberwachung zur Identifizierung gefährlichen Verhaltens geben? Soll die Polizei unter Nutzung privater Datensammlungen einen umfassenderen Datenbestand zur Verhinderung von Kriminalität errichten können? Sollen polizeiliche Daten umfassend durch erkenntnisversprechende Datenverarbeitungsverfahren ausgewertet werden dürfen, um die polizeiliche Aufgabenerfüllung insgesamt zu effektivieren? Solche und weitere Fragen liegen den gesellschaftlichen Aushandlungsprozessen rund um das polizeiliche Informationswesen zugrunde.

Soll das polizeiliche Informationswesen, der Modus polizeilicher Informationsverarbeitung und damit auch die polizeiliche Sozialkontrolle gesellschaftlich regulierbar bleiben, erscheint zunächst nicht in erster Linie relevant, *wie* man Fragen wie die vorstehenden konkret beantwortet. Vielmehr – dem gleichsam vorgelagert – kann man die Frage stellen, ob technologische Entwicklungen von etwas, also von einem Faktor, beeinflusst werden können, der die disparaten und miteinander in manchmal unüberschaubarer Weise interagierenden Einflussgrößen von gesellschaftlicher Technologie-Entwicklung durchdringt, formiert und steuert. Vor dem Hintergrund der dargestellten Heterogenität und Komplexität des polizeilichen Informationswesens scheint es zunächst schwierig, klare Verlaufslinien oder sogar eine konzeptuelle übergeordnete Einflussgröße zu identifizieren, mit denen sich Entwicklungstendenzen dieses sozio-technischen Großsystems aufzeigen lassen.<sup>2156</sup>

Gegen die theoretische Sprachlosigkeit, die in diesen Schwierigkeiten bis zu einem gewissen Grad zum Ausdruck kommt, wenden sich *Jasanoff und Kim* mit ihrem Konzept der „sociotechnical imaginaries“.<sup>2157</sup> Die Idee von sozio-technischen Imaginationen steht auf dem theoretischen Fundament des Menschen als narrativem Wesen. Eines oder sogar das wesentliche Alleinstellungsmerkmal ist danach die Fähigkeit, Narrative gesellschaftlich zu stabilisieren und über die so etablierten kollektiven Vorstellungsbilder gesellschaftliche Prozesse steuerbar zu machen.<sup>2158</sup> An diesen Gedanken

---

2155 Završnik in Završnik (Hrsg.), *Big Data, Crime, and Social Control*, 3 (18).

2156 In diese Richtung etwa Heinrich, *Innere Sicherheit und neue Informations- und Kommunikationstechnologien*, S. 378.

2157 Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*.

2158 Siehe dazu etwa Paumier Jones *The Georgia Review* 50 (1996), 649; Gottschall, *The storytelling animal*; stark popularisiert auch durch Harari, *Sapiens*.

anknüpfend gehen *Jasanoff und Kim* davon aus, dass technologische Entwicklungen von impliziten Vorstellungen darüber durchdrungen sind, was in der sozialen Welt wünschenswert ist, und „collective visions of the good society“ in die soziale Struktur einschreiben.<sup>2159</sup> Damit verbunden sind zwei weitere Überlegungen: Erstens beeinflussen kollektive Werte, die sich gesellschaftlich entsprechend durchsetzen können, die Gestaltung technologischer Systeme. Und zweitens lassen sich an technologischen Projekten normative Entscheidungen hinsichtlich sozialer Ordnung ablesen, worüber spezifische Vorstellungen einer Gesellschaft sichtbar werden können.<sup>2160</sup> Sozio-technische Imaginationen spielen also bei gesellschaftsbeeinflussenden Technologieprojekten, wozu auch der Ausbau des polizeilichen Informationswesens gehört, eine zentrale Rolle: Einerseits stellen sie Leitsterne für die am technologischen Fortschritt beteiligten gesellschaftlichen Systemen dar, nach denen sich die Koordinierung und Mobilisierung von Ressourcen zur Umsetzung der Imagination ausrichten kann. Andererseits reflektieren sozio-technischen Imaginationen gesellschaftliche Selbststeuerungsimpulse, Richtungsentscheidungen und Ordnungswünsche. So wird der sozio-technische Wandel und sein Wertefundament sichtbar, kritisierbar und mit imaginativen Gendarstellungen kontrastierbar.

Aufbauend auf dem Konzept der sozio-technischen Imaginationen sollen die herausgearbeiteten Entwicklungstendenzen des polizeilichen Informationswesens daher zu möglichen Zukunftsszenarien verdichtet werden. Damit soll der wertabhängige Verlauf des informationstechnologischen Wandels bei den deutschen Polizeien und dessen Auswirkungen auf die polizeiliche Sozialkontrolle greifbarer gemacht werden. Nach einer näheren Aufschlüsselung des Konzepts der sozio-technischen Imaginationen (A.) und einigen Bemerkungen zum Szenarien-Design (B.), sollen sodann aus den gegenwärtigen Wandlungsprozessen, wie sie sich insbesondere in den Expert:inneninterviews ausmachen ließen, zwei Szenarien destilliert werden (C. und D.). Beides sind Zukünfte, die von der Warte der grundgesetzlich verfassten Gesellschaft nicht zu befürworten sind. Orientiert wird sich dabei an der Szenarienerstellung von *Gerhold und Brandes*, die dasselbe bereits für Sicherheitstechnologien und ihre Wirkung auf den gesamten Sektor der öffentlichen Sicherheit und damit auch auf das gesellschaftliche

2159 *Jasanoff/Kim* Minerva 47 (2009), 119 (123).

2160 *Chateau/Devine-Wright/Wills* Energy Research & Social Science 80 (2021) (3).

Leben instruktiv vorgemacht haben.<sup>2161</sup> Allerdings sind die hier vorgestellten sozio-technischen Zukünfte gegenüber den Szenarien von *Gerhold und Brandes* zweifach enger gefasst: Es geht erstens nur um einen Ausschnitt des Sektors der öffentlichen Sicherheit und zweitens nur um eine bestimmte – wenn auch fundamentale – Auswirkung auf das gesellschaftliche Leben, die soziale Kontrolle. Kontrastiert werden beide Szenarien sodann mit einem positiven Entwurf für eine weitere Entwicklung des polizeilichen Informationswesens unter dem Eindruck des Massendatenphänomens (E.).

Insgesamt sind die folgenden Ausführungen auch als Synthese der Erkenntnisse und Ergebnisse der Arbeit zu lesen. Die Potenzialität, die aus der Methode des Szenariendesigns spricht, d.h. die vielgestaltigen Möglichkeiten der weiteren Entwicklung polizeilicher Sozialkontrolle, ist dabei eine Folge ihrer multikausalen Bedingtheit. Hier nur eine einzige, definitive Version des Wandels polizeilicher Sozialkontrolle auf der Grundlage der Vorarbeiten zu entwerfen würde sich in unredlicher Weise vor den unterschiedlichen aufscheinenden Entwicklungspfaden verschließen. Gleichzeitig ist das Szenariendesign aber keine exakte Wissenschaft, sodass im Folgenden auch nicht alle denkbaren Wechselwirkungsverhältnisse durchgespielt wurden. Gerade mit Blick auf den qualitativen Aspekt der vorliegenden Untersuchung fügt sich der qualitative Charakter des Szenariendesigns aber in die Vorarbeiten ein. Das gilt umso mehr, als dass die weitere Entwicklung des polizeilichen Informationswesens vor allem auch von menschlichen Entscheidungen abhängt und nicht nach naturwissenschaftlichen Gesetzmäßigkeiten verläuft. Insofern geht es auch nicht um die Akkuratheit der Szenarien im Sinne einer möglichst zutreffenden Vorhersage, sondern um das Aufzeigen von in gegenwärtige Entscheidungen mit einzubeziehende Entwicklungsmöglichkeiten:

„Whether or not a given hypothesized future will actually manifest is not the essential matter. Rather, the aim is to shed light on possible development paths in order to facilitate present-day decisions that will lay the groundwork for a desired future to occur.“<sup>2162</sup>

---

2161 *Gerhold/Brandes* Eur J Futures Res 9 (2021), wobei auch bei ihnen die Polizei eine zentrale Rolle einnimmt. Interessanterweise sind einige Überlegungen zur Polizei im Rahmen des von ihnen als Rückschritt betrachteten Szenarios schon gegenwärtige Polizeipraxis.

2162 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (2).

Das gilt umso mehr, als technologische Entwicklungen stets auch unbeabsichtigte Nebeneffekte zeitigen können, die in der modernen Gesellschaft, die sich vor allem durch komplexe Wechselwirkungsverhältnisse auszeichnet, nur schwer nachzuvollziehen sind. Einmal eingeführt sind Technologien aber beharrend.<sup>2163</sup> Daraus ergibt sich eine prekäre Situation für die Regulierung von risikobehafteten Technologien: Die tatsächlichen Wirkungen technologischer Innovationen zeigen sich erst, wenn sie in die soziale Struktur eingewoben sind, aber die dann wirkenden Beharrungskräfte machen es erforderlich, möglichst zuvor schon problembehaftete Aspekte der Technologie regulativ zu adressieren.<sup>2164</sup> Auf Grundlage des positiven sozio-technischen Zukunftsszenarios sollen abschließend Regulierungspfade aufgezeigt werden (F.).

#### A. Sozio-technische Imaginationen der (Spät-)Moderne

Sozio-technische Imaginationen entstammen, wie das bereits erwähnte Konzept der Sozio-Technizität technologischer Artefakte, den Science & Technology Studies.<sup>2165</sup> Während die Idee der Sozio-Technizität vor allem darauf abzielt, die soziale Bedingtheit von Technologien, also auch ihre Nicht-Determiniertheit, zu ergründen, beschäftigen sich die Science & Technology Studies auch mit der umgekehrten Perspektive, das heißt, wie Technologien auf das soziale Gefüge in all seinen Ausprägungen zurückwirken können. Dabei erteilt diese wissenschaftliche Strömung der Idee eines einseitigen Beeinflussungsverhältnisses eine Absage.<sup>2166</sup> Vielmehr hat sich mit dem Konzept der Koproduktion („co-production“) die Idee eines gegenseitigen, hin-und-herschaukelnden Wechselwirkungsverhältnisses entwickelt. Technologien bedingen sozialen Wandel, aber sozialer Wandel bedingt umgekehrt auch die technologische Entwicklungen.<sup>2167</sup> Oder in den Worten *Jasanoffs*:

---

2163 Das gilt *Bailey/Barley* Information and Organization 30 (2020) zufolge insb. für "intelligente" Informationstechnologien; siehe dazu auch *Collingridge*, The social control of technology, 47 ff.

2164 *Lutz*, Das Ende des Technikdeterminismus und die Folgen: soziologische Technikforschung vor neuen Aufgaben und neuen Problemen, S. 38 f.

2165 Siehe dazu bereits oben S. 68 f.

2166 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), Dreamscapes of modernity, 1 (2).

2167 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (1).

„Briefly stated, co-production is shorthand for the proposition that the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it. Knowledge and its material embodiments are at once products of social work and constitutive of forms of social life; society cannot function without knowledge any more than knowledge can exist without appropriate social supports. Scientific knowledge, in particular, is not a transcendent mirror of reality. It both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments, and institutions – In short, in all the building blocks of what we term the social. The same can be said even more forcefully of technology.”<sup>2168</sup>

Allerdings lässt sich mit dem Konzept der Koproduktion mehr verstehen als erklären. Warum es etwa zur Ausformung spezifischer technologischer Entwicklungen bei ähnlichen sozialen Bedingungen kommt, lässt sich damit nur begrenzt beleuchten.<sup>2169</sup> Diese theoretische Sprachlosigkeit konzeptuell zu überwinden versucht die Idee der sozio-technische Imagination. Ursprünglich für die nationalstaatliche Ebene entwickelt,<sup>2170</sup> hat sich das Konzept davon mittlerweile gelöst und lässt sich durch eine variabelere gesellschaftliche Verortung – auf kleinere Kollektive oder sogar Individuen – erkenntnisgewinnbringender als theoretische Ressource nutzen. So können mehrere Imaginationen innerhalb einer Gesellschaft koexistieren, sowohl in Spannung als auch in einem produktiven Verhältnis zueinander. Ob oder inwiefern sich derartige Imaginationen zukünftiger technologischer Konfigurationen gegenüber anderen durchsetzen, hängt vor allem von gesellschaftlichen Machtverhältnissen ab. So obliegt es oft dem Gesetzgeber, den Gerichten, den Medien oder anderen Institutionen mit gesellschaftlicher Macht, bestimmte Zukunftsvorstellungen über andere zu stellen und sie so im politischen Prozess voranzubringen. Insofern kommen *Jasanoff und Kim* zu folgender Definition sozio-technischer Imaginationen:

„Taking these complexities into account, we redefine sociotechnical imaginaries in this book as collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared un-

---

2168 *Jasanoff* (Hrsg.), *States of knowledge*, 2 f.

2169 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 1 (3)

2170 *Jasanoff/Kim* *Minerva* 47 (2009), 119.

derstandings of forms of social life and social order attainable through, and supportive of, advances in science and technology”<sup>2171</sup>

Besondere Betonung erfährt dabei das Wort „desirable“, weil Projekte, die sozio-technische Zukünfte verwirklichen wollen, regelmäßig auf Visionen aufbauen, die sozialen Fortschritt technologisch erreichen wollen. Damit ist – auf der Kehrseite – stets auch das Gegenteil, also unerwünschte Zukünfte, Teil von sozio-technischen Imaginationen, als Angst vor den gesellschaftlichen Folgen, die bei Durchführung des technologischen Innovationsprozesses eintreten oder aber beim Unterlassen der Innovation. Sozio-technische Imaginationen oszillieren also zwischen den Utopien technologischer Verheißungen und den Dystopien technologischer Abgründe.<sup>2172</sup>

Während sozio-technische Imaginationen häufig auf einzelne als visionär angesehene Personen zurückgehen, brauchen sie den intersubjektiven Halt vieler Mitglieder einer sozialen Gemeinschaft, um in der gesellschaftlichen Struktur wirksam werden zu können.<sup>2173</sup> So war etwa *Horst Herold* als Visionär eines kybernetischen Informationswesens der Polizei zur Steuerung gesellschaftlicher Prozesse im Zusammenhang mit Devianz zwar der Anstoß für viele Projekte der Elektronisierung innerhalb der deutschen Polizei in den 1970er Jahren. Dabei war er jedoch stark auf eine verbreitete Technikeuphorie im polizeilich-sicherheitspolitischen Feld angewiesen, wie sie generell bezeichnend für das sozialliberale Fortschrittsjahrzehnt und den historischen Endpunkt der *trente glorieuses* war. *Herolds* visionäre Kraft verblasste und verlor ihre Wirkkraft dann auch im Angesicht des heraufziehenden Datenschutz-Paradigmas und der Ablehnung eines zu sehr zentralisierten polizeilichen Informationswesens, was sich in einer sozio-technischen Imagination verdichtete, in deren Zentrum die gesellschaftliche Angst vor einem zu mächtigen polizeilichen Überwachungs- und Kontrollapparat stand.<sup>2174</sup>

Dieses Beispiel zeigt auch, dass sozio-technische Imaginationen ein gesellschaftliches Handlungsfeld (geworden) sind, in dem verschiedene Akteur:innen – mal mehr, mal weniger intentional – über die Vorzüge und Nachteile konkreter Vorstellungen verhandeln. Individuen und Kollektive stecken auf diese Weise Gebiete in großen sozio-technischen Möglichkeits-

---

2171 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 1 (4).

2172 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 1 (4 f.).

2173 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 1 (6).

2174 Siehe zu dieser Entwicklung bereits oben S. 130 f.

räumen ab und schaffen damit handlungsleitende Pfadabhängigkeiten.<sup>2175</sup> So wird etwa im sicherheitspolitischen Diskurs von Seiten der Befürworter:innen die Einführung bestimmter technologischer Strukturen zur Terrorismusbekämpfung gefordert, wobei die Angst vor einer technologischen Rückständigkeit der Polizei und der davon ausgehenden Gefahr für die dann vor Terror ungeschützte Gesellschaft als sozio-technische Imagination katalysierend auf Entscheidungsträger:innen wirkt. Umgekehrt bringen Kritiker:innen dagegen die Angst vor einem polizeilich gestützten Überwachungsstaat und vor der Erosion bürgerlicher Freiheiten als Folge technischer Aufrüstung der Sicherheitsbehörden in Stellung.

Der Möglichkeitsraum sozio-technischer Imaginationen ist dabei äußerst weit, aber wohl auch in großen Teilen unsichtbar. Denn die Blicke der Gesellschaft für das, was möglich ist, sind durch die eingeübte soziale Ordnung – bei einigen mehr als bei anderen – konditioniert. Soziale Ordnung ist auf einer grundlegenden Ebene nichts anderes als eine kulturell konditionierte Wahrnehmung der Realität.<sup>2176</sup> Eine Durchbrechung dieser Konditionierung durch neue Vorstellungen davon, was ist und sein sollte, kann also eine soziale Umordnung bewirken – sowohl mit positiven als auch mit negativen gesellschaftlichen Auswirkungen.<sup>2177</sup> Insofern sind sozio-technische Imaginationen auch immer mit der Frage nach gesellschaftlicher Macht verbunden.<sup>2178</sup> Die Imaginationen konkurrieren um eine Hegemonialstellung, auch wenn in der technischen Materialisierung eines Projekts verschiedene gegenläufige Vorstellungen wirksam werden können. Kompromisse zwischen Effektivierung und Begrenzung polizeilicher Sozialkontrolle werden etwa an der datenschutzrechtlichen Sicherung im Rahmen der Einführung neuer Technologien bei der Polizei sichtbar. Technologische Innovationsprojekte sind insofern aber immer ideologisch und politisch.<sup>2179</sup>

Der politische Diskurs verlangt dafür, dass eine Imagination überhaupt anschlussfähig werden und bleiben kann, eine kontinuierliche Anstrengung von Befürworter:innen, mittels derer sich das sozio-technische Imaginativ stabilisieren und in technischen und anderen sozialen Strukturen ein-

---

2175 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (8).

2176 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (14).

2177 Dabei wäre natürlich die Perspektive, aus der die Bewertung „positiv“ und „negativ“ vorgenommen wird, näher zu charakterisieren. Hier geht es jedoch nur um die abstrakte Ebene dieser Dynamik.

2178 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (18).

2179 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (19).



schreiben kann, worüber dann auch wiederum gesellschaftliche Ordnungen gestützt werden können: „An imaginary is neither cause nor effect in a conventional sense but rather a continually rearticulated awareness of order in social life [...] and a resulting commitment to that order’s coherence and continuity.“<sup>2180</sup>

Wie bereits eben angedeutet, spiegelt sich diese sozio-technisch beeinflusste Ordnung in besonderer Weise im Recht, wo die jeweiligen Praktiken und Ordnungsentwürfe unterschiedlicher sozio-technischer Imaginationen aufeinanderprallen. Hier ist es dann an den Richter:innen und Gesetzgebern, auf Grundlage der vorgebrachten Argumente die hegemoniale Stellung bestimmter Vorstellungen auszubauen oder zu schwächen.<sup>2181</sup> Für den vorliegenden Kontext dürfte das Volkszählungsurteil als Grundsatzentscheidung in der Frage nach dem Ausmaß eines datengestützten staatlichen Steuerungsanspruches gelten. Im Urteil stärkten die Richter:innen Ende 1983 eine sozio-technische Imagination, die in der unbeherrschten Datenverarbeitung durch moderne Informationstechnik ein unkalkulierbares Risiko für eine freiheitliche Gesellschaft sah. Verdichtet wurde diese unerwünschte Vorstellung im Bild des informationell selbstbestimmten Individuums, das seither Grundstein für die sich entfaltenden Datenschutzdogmatik ist, welche die Imagination rechtlich operationalisiert und ihr damit gesellschaftliche Wirksamkeit verleihen möchte. Immer wieder wurden aber seitdem auch sicherheitspolitische Technologieprojekte der konkurrierenden Imagination vorgebracht. In der als zunehmend unübersichtlich und ordnungslos wahrgenommenen Gesellschaft der Spätmoderne soll eine Expansion der polizeilichen Datenverarbeitungsfähigkeiten und -kompetenzen die polizeiliche Handlungsfähigkeit und damit die Produktion sozialer Ordnung durch die Polizei aufrechterhalten. Die vielen verfassungsrechtlichen Auseinandersetzungen über den Stellenwert der jeweiligen Imagination haben das Ideal informationeller Selbstbestimmung mittlerweile stark relativiert und das polizeiliche Datenschutzrecht ausgehöhlt. Hat der Datenschutz auch neuen Auftrieb durch die EU-Datenschutzreform von 2016 erfahren, so bleibt die Ausgestaltung des Verhältnisses beider Imaginationen ein „Kampf ums Recht“.<sup>2182</sup> Dabei kann aber gerade die Konkurrenz zweier Imaginationen die Schaffung neuer Vorstellungen stimulieren.<sup>2183</sup>

---

2180 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (26).

2181 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 1 (26).

2182 Jhering, *Der Kampf ums Recht*.

2183 Jasanoff in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 321 (337).

Sozio-technische Imaginationen der Ausgestaltung polizeilicher Sozialkontrolle im Zeitalter der Massendaten bleiben insofern ein Vehikel für die Neugestaltung und Neukalibrierung der gesellschaftlichen und menschlichen Zukunft.<sup>2184</sup> Eine Analyse der sozio-technischen Imaginationen ermöglicht insofern eine tiefgreifende Reflexion über die Perspektiven einer Gesellschaft auf ihre Zukunft und auch über dabei bestehende blinden Flecken. Damit sollte – im besten Fall – das schöpferische Potenzial des Technologie-Einsatzes im Namen der Gesellschaft freigelegt und eingängig betrachtet werden, um die sozio-technische Machbarkeit vielfältiger gesellschaftlicher Welten sicht- und praktikierbar zu machen.<sup>2185</sup>

### B. Szenarien-Design

Bevor die benannten Szenarien breiter dargestellt werden, muss noch über das Szenarien-Design, das eine Methode der Zukunftsforschung ist, gesprochen werden. Wie bereits erwähnt, wird für die folgenden Entwicklungspfade der Polizei als Institution der formellen Sozialkontrolle eine Arbeit von *Gerhold und Brandes* als Ausgangspunkt genommen.<sup>2186</sup> Deren Szenarien-Entwicklung für die Zukunft des Technologie-Einsatzes im öffentlichen Sicherheitssektor in den nächsten 10 bis 15 Jahren und die daraus folgenden Auswirkungen für das gesellschaftliche Leben haben bereits zwei kondensierte Verlaufspfade hervorgebracht. Da die Polizei als wichtigste einzelne Institution im Feld öffentlicher Sicherheit gelten dürfte, weisen beide Szenarien bereits eine hohe Dichte an Überlegungen und fundierten Spekulationen, gewissermaßen „educated guesses“, auch zur Polizei auf. Mit den in der vorliegenden Studie herausgearbeiteten theoretischen, rechtswissenschaftlichen und empirischen Aspekten sollen die von *Gerhold und Brandes* konstruierten Entwicklungslinien der Polizei ergänzt oder aber auch korrigiert werden. Vor allem die qualitative Natur der Szenarien-Methode ermöglicht eine Zusammenführung mit den erarbeiteten Erkenntnissen der Interviewstudie.

Das Konstruieren von Szenarien zielt dabei zunächst einmal darauf ab, Elemente, die als einflussreich für zukünftige Entwicklungen identifiziert worden sind, im Rahmen eines systemischen Vorgehens in konsistente,

---

2184 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 1 (27).

2185 *Jasanoff* in *Jasanoff/Kim* (Hrsg.), *Dreamscapes of modernity*, 321 (339).

2186 *Gerhold/Brandes* *Eur J Futures Res* 9 (2021).

plausible und leicht zugängliche Bilder möglicher Zukünfte zu übersetzen.<sup>2187</sup> Szenarien sind also „logical, plausible and realistic situations based on today’s knowledge, therefore giving an approximate idea of how the future may look.“<sup>2188</sup> Ob eine solche Zukunft tatsächlich eintritt, ist hingegen immer ungewiss,<sup>2189</sup> sodass im Folgenden auch keine Aussagen über die Wahrscheinlichkeit des einen oder anderen Szenarios getroffen werden. Wie bei *Gerhold und Brandes* ist das Ziel der Szenarien-Entwicklung greifbare Bilder der Zukunft zu entwerfen, „which allows the reflection of current debates about security technologies and can inform which actions in the present are best-suited to bringing about desired future states.“<sup>2190</sup> Insofern wird der Wert der Szenarien vorliegend vor allem auch in der Unterstützung beim Finden einer sinnvollen Regulierungsrichtung für das polizeiliche Informationswesen gesehen.

Für die Konstruktion der Szenarien werden in erster Linie die gegenwärtigen technologischen Entwicklungen im polizeilichen Informationswesen herangezogen. Eine zentrale Rolle spielt dabei aber nicht nur die eingesetzte oder auch nicht eingesetzte Technik an sich, sondern auch der organisatorische Umgang der Polizei mit technologischen Innovationen und den Herausforderungen, die sich daraus für die Institution und das polizeiliche Arbeitsfeld stellen. Daneben ist vor allem der rechtliche Rahmen relevant, da normative Rahmenbedingungen Technikentwicklung anleiten, konkret also begrenzen oder freisetzen können. Inwiefern die Polizei in ihren Aufgaben und Befugnissen durch das Recht eingehegt ist, wird eine zentrale Stellschraube für die Form ihrer weiteren informationellen Technisierung sein.<sup>2191</sup> In Bezug auf den bereits begonnenen oder geplanten Technologie-Einsatz sollen explizit auch unerwünschte, nicht bezweckte Effekte der informationstechnologischen Evolution<sup>2192</sup> bei den Polizeien miteinbezogen werden, auch wenn deren Identifizierung sich sachgemäß als schwierig ge-

2187 So *Gerhold/Brandes* Eur J Futures Res 9 (2021) (7); siehe auch K. Steinmüller in Popp (Hrsg.), Zukunft und Wissenschaft, 101; *Lindgren/Bandhold*, Scenario planning.

2188 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4).

2189 *Gerhold/K. Steinmüller* in Peperhove/K. Steinmüller/Dienel (Hrsg.), Envisioning Uncertain Futures, 69 (71).

2190 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4); siehe auch *Grishakova/Gramigna/Sorokin* Frontiers of Narrative Studies 5 (2019), 112; *Neuhaus* in *Gerhold/Holtmannspötter/Neuhaus* ua (Hrsg.), Standards und Gütekriterien der Zukunftsfor-schung, 21.

2191 Ähnlich *Gerhold/Brandes* Eur J Futures Res 9 (2021) (6).

2192 *Rammert*, Technik - Handeln - Wissen, 109 et passim.

staltet.<sup>2193</sup> Allerdings müssen auch Technologie-Entwicklung und -Einsatz in der Gesellschaft sozialer Kontrolle unterworfen werden und bleiben,<sup>2194</sup> sodass der verantwortungsbewusste Umgang mit Technik eine möglichst frühzeitige Reflexion über Technikfolgen erforderlich macht.<sup>2195</sup>

Auch bei ausgeprägten Bemühungen um eine möglichst anschlussfähige intersubjektive Objektivität bleibt beim Szenarien-Design, das vorliegend im Sinne seiner qualitativen Ausprägung durchgeführt wird, die forschende, konstruierende Person in den konkreten Prognosen präsent. Wie auch im Rahmen der durchgeführten Interviews sind Entscheidungen während des Forschungsprozesses immer von einem Vorverständnis abhängig, das generell jedes wissenschaftliche Vorhaben – aber qualitative Studien in besonders expliziter Weise – durchdringt und beeinflusst. Diesem unüberwindbaren Fakt lässt sich nur mit Transparenz begegnen. Diese wurde einerseits bereits im Rahmen der Interviewstudie, die ja maßgeblich in die folgenden Szenarien einfließt, durch Offenlegung von Prozess und Reflexionen gewährleistet. Darüber hinaus wurde mit der Darlegung der Vorgehens bei der Konstruktion auch die Transparenz der Szenarien sichergestellt.<sup>2196</sup> Diese Transparenz stellt zwar keine Objektivität her, macht auch die vorgestellten Szenarien weder richtig, aber auch nicht falsch, sondern vor allem diskutabel, was ohnehin ihr eigentlicher Zweck ist. Sie sollen als Debattenimpuls und Diskussionsgrundlage dienen und gerade kritisiert werden. Die Unvollständigkeit und Kritisierbarkeit der Szenarien ist mithin eine ihrer zentralen und intendierten Eigenschaften:

„While the scenarios we have described intend to enable negotiative processes, a scenario development approach can never be suitable for arriving at a final or conclusive assessment of a subject matter. In this way, far from seeking to adopt a specific polemic tact, we aim instead [...] to provide impetus to debates about our collective future.”<sup>2197</sup>

---

2193 Gerhold/Brandes Eur J Futures Res 9 (2021) (3).

2194 Grundlegend dazu Collingridge, The social control of technology.

2195 Gerhold/Brandes Eur J Futures Res 9 (2021) (3).

2196 Siehe zu den methodischen Reflexionen zu den referenzierten Szenarien Gerhold/Brandes Eur J Futures Res 9 (2021) (17).

2197 Gerhold/Brandes Eur J Futures Res 9 (2021) (17 f.).

### C. Erstes Szenario: Die datenmächtige Polizei der Zukünfte

Das erste hier konstruierte Szenario ist das einer datenmächtigen Polizei, die über die Beherrschung der in den datenmäßigen Repräsentationen liegenden Unwägbarkeiten des prospektiven Realitätsverlaufs den Zufall „gezähmt“ hat<sup>2198</sup> – oder das zumindest auf Grundlage einiger Anhaltspunkte für die Effektivitätssteigerung polizeilicher Sozialkontrolle glaubt.<sup>2199</sup> Dafür sind zwei Faktoren, die sich gegenseitig bedingen und durchdringen, also im erwähnten Sinne koproduzieren,<sup>2200</sup> ausschlaggebend: Die technische und organisatorische Bewältigung des Massendatenphänomens, womit auch die Anpassung der Bewältigungsleistungen ans Recht verbunden ist, sowie eine gesellschaftliche Sicherheitskultur,<sup>2201</sup> die der datenmächtigen Polizei im Wesentlichen befürwortend gegenüber steht. Als Sicherheitskultur wird hier in Anlehnung an Daase „die Summe der Überzeugungen, Werte und Praktiken von Institutionen und Individuen verstanden werden, die darüber entscheiden, was als eine Gefahr anzusehen ist und wie und mit welchen Mitteln dieser Gefahr begegnet werden soll“ angesehen.<sup>2202</sup> Es besteht insofern ein recht enger Zusammenhang zwischen Sicherheitskultur und sozio-technischen Imaginationen.

#### I. Sicherheitskultur

Die Sicherheitskultur ist in diesem Entwicklungsverlauf vor allem durch das häufig beschriebene spätmoderne Unsicherheitsempfinden geprägt.<sup>2203</sup> Die pointiert von Beck beschriebene Bewusstwerdung der Gesellschaft über ihre vielfältigen Risiken<sup>2204</sup> hat – das ist mittlerweile hinlänglich beschrieben worden – einen sich selbst verstärkenden Kreislauf in Gang gesetzt, der technisch immer neue Risiken produziert oder auch entdeckt, um dann wiederum mit vor allem technischen Innovationen darauf zu reagieren,

---

2198 *Hacking, The Taming of Chance.*

2199 Dieses Szenario knüpft an das Szenario „To Be Ahead“ von Gerhold/Brandes Eur J Futures Res 9 (2021) (8 ff.) an.

2200 Siehe dazu bereits oben S. 491.

2201 Zu diesem Konzept siehe Gerhold/Brandes Eur J Futures Res 9 (2021) (4); Daase Aus Politik und Zeitgeschichte 2010, 9.

2202 Daase Aus Politik und Zeitgeschichte 2010, 9 (9).

2203 Siehe dazu bereits Fn. 6.

2204 Beck, Risikogesellschaft.

was aufgrund technischer Risiken häufig wieder zum Beginn des Kreislaufs führt. Die dadurch entstandene Risikowahrnehmung wird dabei immer sensibler und weitet sich auf immer neue Risikophänomene aus – unter anderem auch auf alle möglichen Formen der Devianz.<sup>2205</sup> Der Modus der Sicherheitsproduktion wird zunehmend technisch<sup>2206</sup> und etabliert damit Stück für Stück technische Systeme mit dem Zweck der Überwachung und Kontrolle verschiedener Risiken.<sup>2207</sup> Getragen wird dieser gesellschaftliche Komplex von einer sozio-technischen Imagination der Beherrschbarkeit risikoreicher Zukünfte durch exzessiven und expansiven Technologie-Einsatz.<sup>2208</sup> Beabsichtigte Folge dieses sozio-technischen Sicherheitskomplexes, der seine zentrale staatliche Ausprägung im polizeilichen Informationswesen findet, ist also die zunehmende Sammlung von Daten – Informationen – über Risiken mit der Absicht, sie technisierten Überwachungs- und Kontroll- oder auch: Lösungsstrategien zuzuführen.

Diese Sicherheitskultur spiegelt sich auch im Modus, den die Gesellschaft zur rechtlichen Einhegung von neuen Sicherheitstechnologien an den Tag legt. Gerhold und Brandes gehen davon aus, dass Gesetzgeber und sonstige Regulierungsinstanzen nicht in der Lage sind, mit der Geschwindigkeit und Vielfalt der neuen technischen Regulationsobjekte Schritt zu halten.<sup>2209</sup> Schon jetzt sind solche Effekte in den Interviews zur Sprache gekommen. Fehlende oder fehlerhafte Gesetzgebungsaktivitäten erschweren die Tätigkeit der polizeilichen Datenschutzbeauftragten, was den Verselbstständigungstendenzen der informationstechnologischen Infrastruktur und der mit dieser interagierenden Informationspraktiken des polizeilichen Informationswesens Vorschub leistet. Fehlende Regelungskonzepte,<sup>2210</sup> ein nur unzureichend lernfähiges Recht<sup>2211</sup> sowie die Komplexität der bisherigen Rechtslage und föderale Ordnung der Regulierungsinstanzen verhindern in diesem Szenario eine konsistente und vor allem auch verfassungsgemäß einhegende Regulierung des polizeilichen Informationswesens, dass sich deshalb immer weiter aus seinem Regelungsrahmen löst. Die Gesetz-

---

2205 Miller in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 277 (278 f.).

2206 Gerhold/Brandes Eur J Futures Res 9 (2021) (3), sprechen insoweit von einer "technization of security".

2207 Miller in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 277 (278 f.)

2208 Ähnlich auch Miller in Jasanoff/Kim (Hrsg.), *Dreamscapes of modernity*, 277 (278); siehe auch Gerhold/Brandes Eur J Futures Res 9 (2021) (2).

2209 Gerhold/Brandes Eur J Futures Res 9 (2021) (8).

2210 Bäcker, A-Drs. 18(4)806 D, S. 2, 10.

2211 Zur Lernfähigkeit bereits Roßnagel Zeitschrift für Rechtspolitik 1991 (25), 55 (57); Golla Kriminologisches Journal 52 (2020), 149.

gebung beschränkt sich – wie schon jetzt teilweise zu konstatieren ist – zunehmend auf die reine Legitimierung polizeilicher Informationstechnologien und der damit einhergehenden Informationspraktiken. Kriminalitätsrisiken wird von der Sicherheitskultur aber ein größerer Stellenwert zugestanden als abstrakte Risiken für schleichende Freiheitsverluste.

## II. Technologische Entwicklung des Informationswesens

Die Technisierung polizeilicher Sozialkontrolle wird von einer insofern affirmativen Sicherheitskultur getragen. Gleichzeitig wird diese Kultur kaum durch ein normatives Element der Zurückhaltung eingeschränkt, sodass die Grenzen des technisch Möglichen zunehmend die Grenzen des Faktischen im polizeilichen Informationswesens bestimmen.<sup>2212</sup>

Zunächst gelingt den deutschen Polizeien daher der im Rahmen des Projekts Polizei 2020 geplante Umbau des polizeilichen Informationswesens, was die Datenhaltung stark effektiviert. Daten müssen nun regelmäßig nur noch einmal erfasst werden und können dann über entsprechende Programmierungen an die Anwendungen, für die sie jeweils gebraucht werden, gesteuert werden. Die Schaffung eines zentralen Datenbestandes ermöglicht auch einen erkenntnisgewinnbringenderen Einsatz von algorithmengestützten Massendatenverarbeitungsverfahren. Im Zuge des Prozesses, der oben bereits als Datafizierung beschrieben wurde,<sup>2213</sup> meistern die deutschen Polizeien die „zunehmende Nutzung korrelativ fundierter, statistischer Datenanalysen [...], [also] die auf Entscheidungsfindung ausgerichtete und algorithmisch vermittelte (Massen-)Analyse von Daten [...], deren Resultate entsprechend umgesetzt werden und somit die polizeilichen Praktiken nachhaltig prägen.“<sup>2214</sup> Dabei erhält das polizeiliche Informationswesen Unterstützung durch einen großen polizeilich-sicherheitswirtschaftlichen Komplex, der stetig neue Innovationen für verlässliche Abnehmer hervorbringt. Auf einer basalen Ebene effektivieren die verbesserte Datenhaltung und die steigende Kompetenz in der datengestützten Produktion von handlungsleitendem Wissen die polizeiliche Informations-

---

2212 Skeptisch hinsichtlich einer solchen polizeilichen Entwicklung etwa *Krahmer* in Rüdiger/Bayerl (Hrsg.), *Digitale Polizeiarbeit*, 215.

2213 Siehe dazu bereits oben S. 46 ff.

2214 *Egbert* in Hunold/Ruch (Hrsg.), *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung*, 77 (78).

arbeit nachhaltig und eröffnen der polizeilichen Sozialkontrolle damit neue Potenziale.

Gleichzeitig vervielfältigen sich die Kontaktpunkte, die das polizeiliche Informationswesen mit gesellschaftlichen Feldern hat, indem mehr informationstechnische Schnittstellen geschaffen werden, über die lebensweltliche Daten über soziale Konflikte und abweichendes Verhalten direkt in die polizeilichen Datenbestände gelangen können.

Einerseits sind Smartphones alltägliches Einsatzgerät bei der datenmächtigen Polizei. Jeder Einsatz, ob mit vorrangig präventiver oder repressiver Stoßrichtung, wird umfassend und – nach Möglichkeit – granular erfasst und an die polizeilichen Informationssysteme übertragen, von wo dann eine automatisierte Weiterleitung an Stellen und Anwendungen erfolgt, an denen die Daten benötigt werden. Zudem nimmt der Einsatz von automatischen Kennzeichenlesesystemen, Bodycams – auch zu generellen Einsatzdokumentationszwecken – und anderen Formen mobiler und stationäre Videoüberwachung zu. Videoüberwachungssysteme dienen generell als Plattform für Software, etwa zur Verhaltenserkennung und biometrischen Identifikation, sodass sich die informationelle Durchdringung der von den Kameras erfassten Lebenswelt noch einmal erhöht.<sup>2215</sup>

Andererseits erlauben Online-Wachen es den Bürger:innen, über ihre (mobilen) Endgeräte wie Smartphones und Laptops direkt Informationen an die Polizei zu senden. Eine Weiterentwicklung dieser Kommunikationsart ermöglicht das Melden einer Straftat über einen speziellen Kanal, etwa über eine App, woraufhin die Polizei augenblicklich Einsatzkräfte entsenden kann, die sich zuvor über mitgesendete Daten beispielsweise in Form von Videos ein Vorabbild der Lage am Einsatzort machen können.<sup>2216</sup> Daneben werden in großem Maße OSINT-Verfahren und Online-Streifen durchgeführt, mit denen virtuelle Räume zum einen präventiv nach Auffälligkeiten durchsucht werden, zum anderen aber auch digitale Hinweise auf Devianz sowohl im Virtuellen als auch im Analogen registriert werden. Neben den allgemeinen Online-Wachen bestehen institutionalisierte Meldeverfahren für als besonders gesellschaftsschädlich geltendes abweichendes Verhalten im digitalen Raum – „Hate Speech“-Verdachtsfälle etwa werden nach Meldung automatisiert zur Auswertung an die dafür

---

2215 Es wird etwa bereits davon berichtet, dass Bodycams in einigen Ländern mit Gesichtserkennungssoftware ausgestattet werden, siehe dazu *Cheslow Times of Israel* v. 22. Januar 2022.

2216 *Gerhold/Brandes Eur J Futures Res* 9 (2021) (8 f.).



vorgesehene Stelle beim Bundeskriminalamt geleitet, wo Algorithmen die massendatenförmige Online-Kommunikation der Gesellschaft vorfiltern und dann an menschliche Bearbeiter:innen weiterleiten. In einem an dieser Stelle zugespitzten Szenario wäre auch das automatisierte Versenden von Strafbefehlen nach algorithmengestützter Entscheidung über die strafrechtliche Relevanz einer Äußerung ähnlich dem automatisierten Mahnverfahren denkbar.

Neben diesen Dynamiken, welche die Expansion der polizeieigenen Datensammlung betreffen, können die deutschen Polizeien auch zunehmend auf die in der Gesellschaft an anderer Stelle aggregierten Datenakkumulationen zugreifen. Einerseits sind staatliche Daten weitestgehend über einheitliche Datenformate harmonisiert und somit schnell je nach Bedarf austausch- und integrierbar. Daneben besteht zudem die Möglichkeit des bedarfsmäßigen Zugriffs auf die Bestände privater Akteure wie Social Media-Betreiber, Data Broker und sonstige Digitalunternehmen. Dieser Kontakt ist über Schnittstellen technisch verfestigt worden, sodass die Polizei gesellschaftliche Realitäten im Bedarfsfall über die kontextbezogene Integration verschiedener Datenquellen rekonstruieren und darüber Anzeichen für erwartetes oder bereits geschehenes abweichendes Verhalten identifizieren und entsprechend adressieren kann.<sup>2217</sup> In ähnlicher Weise können etwa Smart Home-Geräte und die sonstigen Sensoren der „Onlife“-Welt<sup>2218</sup> ausgewertet und vergangene Lebenssituationen auf diese Weise besser für Zwecke der Strafverfolgung rekonstruiert werden.

Neben diesen Tendenzen der Extensivierung und Effektivierung der technologischen Infrastruktur des polizeilichen Informationswesens verändert sich auch die Interaktion der Polizist:innen mit diesem sozio-technischen Großsystem fundamental. Vor allem anderen macht sich dies in der mobilen Verfügbarkeit der Datenmacht des Informationswesens in den verschiedenen Einsatzkonstellationen bemerkbar, die den Beamt:innen einen starken informationsbasierten Rückhalt und damit einen Wissensvorsprung vor ihrem Gegenüber gewährt. Wie eine solche Zukunft der engmaschigen Integration polizeilicher Einsätze in datenangereicherte Handlungsabläufe aussehen könnte, haben *Bain et al.* beschrieben:<sup>2219</sup>

---

2217 Gerhold/Brandes Eur J Futures Res 9 (2021) (10).

2218 Zum Begriff des „Onlife“ bereits oben Fn. 1272.

2219 Siehe zum Folgenden Bain/Carson/Conser ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (126 ff.).

Zwei Polizeibeamt:innen werden zu einem Fall häuslicher Gewalt geschickt. Ein Sprachassistent gibt über einen auf der Schulter angebrachten Miniatur-Lautsprecher bisher bekannte Informationen zum Einsatzgeschehen durch, die Anfahrt wird durch die auf dem Fahrzeugbildschirm dargestellten GPS-Informationen geleitet. Das Kamerasystem des Fahrzeugs und die Bodycams werden automatisch zu Eigensicherungs- und Dokumentationszwecken aktiviert und ein Live-Video-Feed wird an die Einsatzleitzentrale übertragen. Vor Eintreffen am Einsatzort erfahren die Beamt:innen, dass ein offensichtlich betrunkenener Ehemann seine Frau anschreit und bedroht, dass zwei kleine Kinder in der Wohnung leben, dass der Ehemann in der Vergangenheit wegen häuslicher Gewalt verhaftet wurde und dass eine weitere Einheit entsandt wird. Fotos von allen Bewohner:innen der Wohnung und Kennzeicheninformationen für die auf Ehemann und Ehefrau zugelassenen Fahrzeuge werden an den Computer des Streifenwagens gesendet. Sofort bei Ankunft am Ort des Geschehens scannt das Videosystem des Polizeifahrzeugs die Nummernschilder der vor dem Haus geparkten Fahrzeuge. Ein Fahrzeug gehört der Familie, ein weiteres vor dem Haus abgestelltes Fahrzeug ist auf eine andere Person zugelassen. Name und Bild dieser Person werden an den Bordcomputer des Streifenwagens gesendet. Die Beamt:innen steigen aus und schieben sich ihre Visiere über die Augen, woraufhin das in die Visiere integrierte Heads-up-Display aktiviert wird. Die Displays stellen den Beamt:innen die zuvor an den Bordcomputer gesendeten Informationen zu den Fahrzeugen bereit. Beide Polizist:innen nähern sich der Eingangstür, aus der gerade eine männliche Person auf die Veranda tritt. Auf Ansprache hin äußert der Mann, dass die Polizei nicht gebraucht werde, es sei nur ein herkömmlicher, mittlerweile geklärter Familienstreit gewesen. Die Bodycams tasten Gesicht und Augen der Person ab und übertragen die biometrischen Daten an das polizeiliche Informationswesen, wo sie verarbeitet werden. In Sekundenschnelle wird die Identität der männlichen Person mit einer Wahrscheinlichkeit von 95 % durch einen Datenbankabgleich festgestellt. Ein Bild der identifizierten männlichen Person wird an den Bordcomputer des Einsatzfahrzeugs gesendet und dann wieder an das Display der Visiere übertragen, wo sie das Ergebnis und die Wahrscheinlichkeitsschätzung sichtbar werden. Die Beamt:innen akzeptieren das Ergebnis als korrekt, es ist der Halter des familienfremden Fahrzeugs. Im Hintergrund werden weitere Daten abgeglichen, vorherige Polizeikontakte der Person werden gesucht. Währenddessen haben die Bodycams das Verhalten der familienfremden Person erfasst und analysiert. In der Ecke der polizeilichen Displays beginnt eine rote LED zu blinken. Zwei

Warnungen werden eingeblendet. Einerseits zeigt die Person eine Körpersprache, die auf einen bevorstehenden körperlichen Angriff schließen lässt. Zudem sei aufgrund unbewusster Gesichts- und Körperbewegungen zu erkennen, dass die Person wahrscheinlich lügt. Die Beamt:innen bitten die Person, auf die Straße zu gehen und mit den anderen Polizist:innen zu sprechen, die – worüber mittels des Schulterlautsprechers informiert wird – innerhalb weniger Sekunden eintreffen würden. Die Person leistet der Aufforderung Folge, wird aber bei ihren Bewegungen von den Bodycams erfasst, sodass bei verdächtigem Verhalten wie dem Abweichen vom Kurs eine Alarmmeldung erfolgen kann. Während ein Beamter vor dem Haus verbleibt, betritt seine Kollegin die Wohnung und spricht mit dem Mann und der Frau. Während der Interaktion zwischen (mutmaßlichem) Täter und Opfer bleiben die am Körper getragenen Überwachungssysteme der Beamtin zur Beobachtung der Situation eingeschaltet. Der Ehemann wird wegen Körperverletzung festgenommen, noch am Ort werden Daten an zu beteiligende (staatliche) Stellen wie dem Jugendamt, dem Opferhilfebüro und dem zuständigen Gericht wegen eines Aufenthaltsverbots übertragen. Der festgenommene Ehemann wird vor Ort biometrisch vermessen und die Daten werden samt einer DNA-Probe an das polizeiliche Informationswesen übertragen. Ein eingesprochener Bericht wird automatisiert in Text umgewandelt und mit allen anderen Daten, die beim Einsatz angefallen sind, an das polizeiliche Vorgangsbearbeitungssystem übertragen, von wo die Daten dann an die entsprechenden Anwendungen gesteuert werden. Abschließend wenden sich die Beamt:innen noch an die Social-Media-Seite ihrer Polizeibehörde und informieren so die örtliche Gemeinschaft über den Vorfall und den Ausgang des Einsatzes.

Die anhand dieses hypothetischen Fallbeispiels beschriebenen Potenziale des polizeilichen Technologie-Einsatzes zeichnen sich vor allem durch die Eigenschaften der Kombination und Synergie aus. Die Möglichkeiten, die sich daraus ergeben, sind vielfältig und in ihren Kontrolleffekten tiefgehend. So ist etwa auch denkbar, dass über mobile Endgeräte flächendeckend über Apps auf die automatisierte Datenanalyse zugegriffen werden kann, womit die informationelle Macht der Polizei bei Kontakt mit Personen massiv gesteigert würde – die Implikationen werden bereits im geschilderten Beispiel deutlich: Ein Objekt – das familienfremde Fahrzeug – wird in seiner Verknüpfung zu einer Person angezeigt, über die wiederum Erkenntnisse zu vorheriger Delinquenz zur Verfügung gestellt werden können. Auch der Streifenwagen wird bei der datenmächtigen Polizei zu einer

Plattform für weitere Technologien: Die installierten Kameras könnten schlicht dauerhaft Kennzeichen lesen und bei Trefferfällen eine Benachrichtigung an die Besatzung des Wagens senden – samt entsprechend verfügbarer Datenverknüpfungen zum in Frage stehenden Kennzeichen bzw. Fahrzeug. *Brayne* beschreibt diesen Wandel von einer auf aktives Suchen und Identifizieren gerichteten hin zu einer von automatisierten Alarmen geleiteten Polizeiarbeit bereits konkret für das Los Angeles Police Department und sieht darin eine emblematische Entwicklung der massendatengestützten Polizeiarbeit.<sup>2220</sup>

Im Szenario der datenmächtigen Polizei verschränken sich also menschliches und maschinelles Wahrnehmen, zu einer Hybridform, was vor allem die Frage nach der menschlichen Handlungsmacht aufwirft. Was soll passieren, wenn die Verhaltenserkennung einen erheblichen Angriff detektiert? Denkbar wäre es, dass – wenn die angreifende Person auch auf Aufforderung nicht ablässt und weitere Gefahrenparameter überschritten werden – eine automatisierte Verteidigungshandlung von der insoweit „intelligenten“ Ausrüstung der Beamten:innen ausgeführt wird, etwa in Form eines Elektroschocks oder Pfeffersprays. Die Bediensteten der datenmächtigen Polizei wären in einem solchen Fall keineswegs auch datenmächtige Polizist:innen, sondern vielmehr instrumentelle Ausformungen des sozio-technischen Informationswesens.<sup>2221</sup>

Mit der zumindest graduellen Übersteuerung des individuellen Polizist:innenverhaltens würde polizeiliches Handeln in der Breite zunehmend homogenisiert. Divergierende Interpretationen anlässlich des Verhaltens von Personen würden mehr und mehr einer durch technische Instrumente programmierten Reaktion auf abweichendes Verhalten weichen,<sup>2222</sup> wobei dies aufgrund der potenziellen Diskriminierungsanfälligkeit von algorithmengestützten (Massen-)Datenverarbeitungsverfahren nicht zwangsläufig einen Gerechtigkeitszuwachs bedeuten würde.

Allerdings schafft die Datafizierung mit ihrer Durchdringung des polizeilichen Arbeitsalltags auch neue Potenziale für eine öffentliche Kontrolle, etwa durch die Veröffentlichung von Videomaterial aus Polizeieinsätzen zur Ansicht durch die Bürger:innen. Auch die einsatzgestaltenden Entschei-

---

2220 *Brayne*, Predict and surveil, S. 45 f.

2221 *Bain/Carstone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (121 f.).

2222 *Bain/Carstone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (123).

dungen selbst sind durch die starke technische Rahmung detaillierter nachvollzieh- und damit überprüfbar.<sup>2223</sup> Allerdings setzt eine solche Kontrolle voraus, dass es noch einen hinreichend konkreten normativen Rahmen gibt, der ein solches Kontrollregime überhaupt fordert und der Kontrolle inhaltliche Anhaltspunkte liefert. Denkbar wäre vor allem eine organisatorische Absicherung der informationellen Maßnahmen der datenmächtigen Polizei durch human in the loop-Verfahren, um möglichst viele Fehlidentifizierungen und damit verbundene unrechtmäßige Persönlichkeitsbeeinträchtigungen zu vermeiden<sup>2224</sup> sowie um die Legitimität der technikgestützten Sozialkontrolle nicht allzu stark erodieren zu lassen.

### III. Polizeiliche Sozialkontrolle

Die Datenmacht der Polizei übersetzt sich im hier beschriebenen Entwicklungspfad in eine gegenüber der heutigen Situation intensivierten Sozialkontrolle. Dabei wären die Wandlungsprozesse der polizeilichen Sozialkontrolle wohl nicht auf eine der vier oben beschriebenen Dynamiken (totaler oder umfassender, selektiver, sanfter, härter) beschränkt,<sup>2225</sup> da es nach wie vor sehr heterogene Kontexte gibt, in denen die Polizei über ihr Handeln soziale Ordnung wiederherstellt oder aufrechterhält.

Durch ihre verbesserten Fähigkeiten in Datengenerierung, Datenhaltung und Datenverarbeitung dürfte die polizeiliche Sozialkontrolle in erster Linie umfassender werden. Wenn durch das Anwachsen entsprechender Schnittstellen mehr Informationen über soziale Konflikte und abweichendes Verhalten in das polizeiliche Hellfeld gelangen, wo sie dann auch effektiver verarbeitet werden können, steigt die Zahl der bekanntgewordenen Fälle abweichenden Verhaltens sowie die entsprechende Verhinderung oder Sanktionierung dieses Verhaltens. Durch die generelle Anwendung von algorithmengestützten Massendatenverarbeitungsverfahren innerhalb der Polizei kann nach datenförmigen Mustern von Devianz in den informationellen Repräsentationen von lebensweltlichen Phänomenen gesucht werden. Sowohl retrospektiv als auch proaktiv können zunehmend Kriminalitätsmuster in den aus verschiedenen Quellen zusammengeführten Datensätzen identifiziert werden. Die Polizei wird damit in die Lage

---

2223 Gerhold/Brandes Eur J Futures Res 9 (2021) (11).

2224 Gerhold/Brandes Eur J Futures Res 9 (2021) (10).

2225 Siehe dazu bereits oben unter S. 87 ff.

versetzt, aggregiertes gesellschaftliches Verhalten auf Irregularitäten und Abweichungen hin zu untersuchen, Kriminalitätsursachen zu ergründen und – im „Idealfall“ – neue Kriminalitätsphänomene bei ihrer Entstehung zu beobachten. Diese polizeiliche Form der Massendatenproduktion und -verarbeitung macht es quasi unmöglich, sich dauerhaft dem staatlichen Blick zu entziehen, da die Teilhabe an der Gesellschaft und ihren Einrichtungen das Hinterlassen digitaler Spuren erforderlich macht.<sup>2226</sup> Zwar gibt es weiterhin solche, die mit technologischen Mitteln ihrer Identifizierung und Dingfestmachung entgehen können, aufgrund der dafür erforderlichen Expertise trifft dies allerdings nur auf einen geringen Teil der Delinquenten und auf einen noch geringeren Teil der Gesamtgesellschaft zu. Vermisste Personen gehören der Vergangenheit an, gesuchte Personen werden zu- meist umgehend verhaftet.<sup>2227</sup> Damit einher geht zudem eine ausgeweitete Zuständigkeit der Polizei für abweichendes Verhalten, da sie die entsprechenden technischen „Lösungen“ dafür in Form des stark ausgeweiteten Informationswesens zur Hand hat.<sup>2228</sup> Die Polizei ist (weiterhin) der zentrale Knotenpunkt im Netzwerk staatlicher Sozialkontrolle. Insgesamt schwingt in dieser zunehmend umfassender werdenden Sozialkontrolle die implizite Grundphilosophie der uneingeschränkten Befürworter:innen des Massendatenparadigmas mit: Wenn nur genug Daten gesammelt sind, wird handlungsleitendes Wissen über bisher unverstandene oder gänzlich unbekannte gesellschaftliche Prozesse generiert werden können,<sup>2229</sup> was sich in eine sozio-technische Vision der datengestützten Steuerung und Neutralisierung von Verhaltensdivergenzen übersetzt. In der so imaginierten Gesellschaft wird es weiterhin bestimmte Kriminalitätsphänomene geben, diese sind aber durch massendatenbasierte Wissensproduktion und darauf aufbauende Kriminalitätskontrollmechanismen sehr viel stärker eingeeht als dies gegenwärtig der Fall ist.<sup>2230</sup> Aufgrund der Ubiquität von als Kriminalität etikettiertem abweichendem Verhalten in der Gesellschaft<sup>2231</sup> bedeutet die Ausweitung des polizeilichen Blickes zugleich die zunehmende Erfassung und datenförmige Repräsentation von Gesellschaftsmitgliedern in den poli-

---

2226 Gerhold/Brandes Eur J Futures Res 9 (2021) (9).

2227 Gerhold/Brandes Eur J Futures Res 9 (2021) (10).

2228 Gerhold/Brandes Eur J Futures Res 9 (2021) (9).

2229 Mayer-Schönberger/Cukier, Big Data; Anderson, The end of theory: The data deluge makes the scientific method obsolete.

2230 Egbert/Leese, Criminal futures, S. 56.

2231 Farrall/Karstedt, Respectable citizens - shady practices.

zeilichen und strafjustiziellen Informationssammlungen, wie es sich in den Vereinigten Staaten bereits abzeichnet.<sup>2232</sup>

Innerhalb dieser engmaschigen polizeilichen Sozialkontrolle wird die Polizei voraussichtlich – trotz affirmativer Sicherheitskultur – mit Ressourceneingpässen zu kämpfen haben, sodass eine Priorisierung des Ressourceneinsatzes nach wie vor geboten sein wird. Aufgrund der umfassenden Datenbasis des Informationswesens und der darauf aufbauenden leistungsstarken Algorithmen der massendatengestützten Wissensproduktion kann die Polizei allerdings im Wege des personen- und raumbezogenen Predictive Policing besonders gefährliche Individuen und Orte effektiver identifizieren und kontrollieren.<sup>2233</sup> Insofern wird die polizeiliche Sozialkontrolle gleichzeitig – und scheinbar paradoxerweise – totaler und selektiver. Erst durch eine Ausweitung des polizeilichen Hellfeldes, das heißt der für die Wissensproduktion benötigten Datenbasis, kann die Polizei jedoch überhaupt mit größerer Sicherheit Prognosen darüber treffen, ob eine Person oder ein Ort im Vergleich besonders gefährlich ist oder nicht. Die Selektivität massendatenvermittelter Sozialkontrolle durch die Polizei baut mithin auf einer umfassenderen Datenerfassung und -verarbeitung auf.<sup>2234</sup>

Zudem gibt es im Szenario der datenmächtigen Polizei auch Anhaltspunkte dafür, dass die ausgeübte polizeiliche Sozialkontrolle – zumindest auf den ersten Blick und in der Breite – sanfter werden könnte. Einerseits kann die Massendatenverarbeitung schon frühzeitig Muster gerade beginnender oder zu erwartender Kriminalität identifizieren, was der Polizei – etwa durch Gefährderansprachen und Ähnliches<sup>2235</sup> – ein gleichsam frühzeitiges, aber dafür weniger invasives Eingreifen und Gegensteuern ermöglicht, um entsprechende Kriminalitätsrisiken im Keim zu ersticken oder gar nicht erst aufkommen zu lassen. Zudem ermöglicht auch die Anreicherung der Lebenswelt mit Sensoren frühzeitige(re) oder echtzeitige Interventionen der Polizei in bevorstehenden oder akuten Gefahrensituationen, indem etwa visuelle Sensoren, also Kameras, verdächtiges Verhalten erkennen, softwarebasiert klassifizieren und dann Alarm auslösen können,<sup>2236</sup>

---

2232 Siehe dazu etwa *Brayne*, Predict and surveil, S. 2.

2233 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).

2234 In diese Richtung für den gesamtgesellschaftlichen Zusammenhang auch *Chriss*, Social Control, S. 211 ff.

2235 Solche – nach deutscher Terminologie – Gefährderansprachen wurden beispielsweise im Rahmen der sogenannten Strategic Subject List („Heat List“) in Chicago praktiziert, siehe dazu etwa *Ferguson*, The rise of big data policing, S. 37 ff.

2236 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).

wodurch auch hier zunächst mit möglichst niedrigschwelligen Maßnahmen der Versuch einer Gefahrauflösung unternommen werden kann.

Allerdings ist bedenkenswert, ob die datenmächtige Polizei nicht auch punktuell Formen härterer Sozialkontrolle hervorbringt. Das ist in zweierlei Hinsicht möglich. Einerseits werden, wie beschrieben, im Rahmen der Selektivierung der massendatenbasierten Sozialkontrolle besonders gefährliche Personen und Orte identifiziert. Da es sich dabei um Individuen und Räume handelt, die – in der relativen Logik des Vergleichs der zur Verfügung stehenden Daten – als die nach jeweils aktuellem Kenntnisstand die *gefährlichsten* für die soziale Ordnung angesehen werden müssen, liegt es nahe, dass die polizeiliche Reaktion hier einigermaßen hart ausfällt, um das wahrgenommene Risiko möglichst effektiv zu eliminieren. Zwar ist damit noch nicht unbedingt eine unterwerfende Sozialkontrolle im Sinne *Beydouns*<sup>2237</sup> beschrieben. Andererseits ist, gewissermaßen an die Unterseite der sanften Sozialkontrolle angeheftet, eine Entwicklung denkbar, die sich gegenüber Teilen der Gesellschaft als strengere Sozialkontrolle äußert:

„The control in this algorithmic world is not a control that guides you against some presumed, autonomous will. Instead it's a control that frames your world. It conditions the possibilities available for you to live your life as a user - as well as a member of a category.”<sup>2238</sup>

In einer Gesellschaft, in der Teilhabe am Gemeinwesen über die Preisgabe von Daten vermittelt wird, in der die soziale Ordnung zunehmend über Algorithmen der Risikoidentifizierung und -kategorisierung hergestellt wird, werden diejenigen, die sich davor fürchten, dass ihr abweichendes und eventuell auch strafrechtlich relevantes Verhalten bekannt wird und zu Nachteilen für sie führt, weniger am gesellschaftlichen Leben teilhaben können.<sup>2239</sup> Die Massendatenüberwachung wirkt so gesamtgesellschaftlich gesehen negativ auf die ohnehin schon ungleiche Verteilung von Lebenschancen im Digitalzeitalter.<sup>2240</sup> Vermeidendes Verhalten und Verdrängungseffekte schaffen so eine Klasse von digital von der Gesellschaft Ausgegrenzten. Zugespißt formuliert könnte man darin eine Form der digital vermit-

---

2237 Siehe dazu bereits oben unter S. 98 f.

2238 *Cheney-Lippold*, We are data, S. 148.

2239 *Haggerty/Ericson* Br J Sociol 51 (2000), 605 (619); *Brayne* Am Sociol Rev 79 (2014), 367.

2240 *Brayne*, Predict and surveil, S. 148.



telten Verbannung oder Internierung sprechen.<sup>2241</sup> Auch ist zu bedenken, dass eine Intensivierung der polizeilichen Sozialkontrolle die Polizei nicht zu einer Institution macht, die plötzlich die Ursachen von Kriminalität wirksam beheben kann. Zu erwarten bleibt vielmehr, dass auch die datenmächtige Polizei weiterhin nur die Konsequenzen sozialer Probleme in Form von Kriminalität und Unordnung bekämpft, ohne den Versuch zu unternehmen, Ihnen das Substrat zu entziehen und wirksame sozialpolitische Interventionen zu betreiben.<sup>2242</sup>

Insgesamt könnte diese gewandelte polizeiliche Sozialkontrolle auch über die beschriebenen Effekte hinaus gesamtgesellschaftliche und wohl ungewollte Nebenwirkungen auslösen. So meint *Moore*, „[i]f we reduced crime, but did so by relying on more intrusive investigative techniques, or patrol techniques that were both more assertive and viewed as biased, then the increased use of authority would have to be viewed as a loss to be put against the gain.“<sup>2243</sup> Auch sind vor diesem Hintergrund sich aufschaukelnde Auswirkungen auf gesellschaftliche Interaktionen rund um die soziale Ordnung denkbar: Führt etwa eine als zu eng empfundene Sozialkontrolle zu einem zunehmenden Verlust der Legitimation der Polizei, könnte es als Reaktion auf diesen Legitimationsverlust zu stärkeren sozialen Unordnungsphänomenen kommen, die dann wiederum eine Intensivierung der (polizeilichen) Sozialkontrolle hervorrufen. Überhaupt wäre fraglich, was für eine Subjektkultur<sup>2244</sup> eine Gesellschaft ausformen würde, in der die Polizei in der beschriebene Art und Weise soziale Ordnung produziert. Während einerseits die umfassende Sozialkontrolle ein stark diszipliniertes, fremdgesteuertes und normbefolgendes Subjekt plausibel erschienen ließe, wie es noch recht typisch für die 1950er und 1960er Jahre war,<sup>2245</sup> ist mit Blick auf *Popitz* Konzept der Präventivwirkung des Nichtwissens<sup>2246</sup> auch die gegenteilige Tendenz denkbar. Dadurch, dass sich das Subjekt der vielfältigen gesellschaftlichen Normübertretungen gewahr wird, die aufgrund der engmaschigen polizeilichen Sozialkontrolle aufgedeckt sowie dann verhindert oder sanktioniert (oder beides) werden, normalisiert sich

---

2241 So etwa *Leman-Langlois* in Deflem (Hrsg.), *The Handbook of Social Control*, 347 (359); siehe genereller zu dieser Dynamik der Ausgrenzung auch *Singelstein/Kunz*, *Kriminologie*, S. 407 ff.

2242 *Lyon Big Data & Society* 1 (2014), 1-13 (7).

2243 Mark H. Moore, zitiert nach *Brayne*, *Predict and surveil*, S. 143.

2244 Zum Begriff siehe etwa *Reckwitz*, *Das hybride Subjekt*.

2245 *Reckwitz*, *Das Ende der Illusionen*, S. 207 f.

2246 *Popitz*, *Über die Präventivwirkung des Nichtwissens*.

einerseits die gesellschaftliche (Straf-)Sanktion bis zu einem gewissen Grad und andererseits verblasst das Vertrauen des Subjekts in das gesellschaftliche Normsystem zunehmend. Die soziale Normordnung wäre also paradoxerweise geschwächt. Gleichzeitig wäre aber auch sozialer Wandel, der sich *Durkheim* zufolge im Wesentlichen über die Weiterentwicklung des Normbestandes durch Übertretung der Normen materialisiert, gehemmt.<sup>2247</sup>

#### *D. Zweites Szenario: Die überforderte Polizei – Zukunft ohne Polizei*

Das zweite Szenario konstruiert eine Zukunft, in der die Polizei weitgehend überfordert mit dem digitalen Wandel und den gesellschaftlichen Auswirkungen des Massendatenphänomens ist.<sup>2248</sup> Es ist, pointiert formuliert, eine Zukunft ohne Polizei, weniger zugespitzt könnte man auch sagen: mit einer in ihrer gesellschaftlichen Rolle stark herabgestuften Polizei. In diesem Szenario haben sich die gegenwärtigen Entwicklungspotenziale zu einer im Kern vor allem kritischen Sicherheitskultur in der Gesellschaft verdichtet. Die Polizei hat die technisch-organisatorische Anpassung an die neuen gesellschaftlichen und medialen Konfiguration nicht bewältigen können, was zu einer Verkümmern der polizeilichen Sozialkontrolle in wichtigen Bereichen und einem institutionellen Bedeutungsverlust geführt hat.

#### I. Sicherheitskultur

Die bereits heute im Diskurs präsenten Datenschutz-Befürworter:innen sind tonangebend geworden. Bei den deutschen Polizeien ist es immer wieder zu unrechtmäßigen Datenverarbeitungen gekommen: Es wurden polizeiliche Daten zu privaten Zwecken abgerufen und im Rahmen von strafrechtlichen Ermittlungen wurden verbotene Datenverarbeitungsmethoden angewendet. Ohne dass zuvor Rechtsgrundlagen geschaffen worden waren, hatten einzelne Behörden zudem mit neuen, eingriffsintensiven Technologien experimentiert<sup>2249</sup> und damit in für die Betroffenen spürbarer Wei-

---

2247 *Durkheim* in Sack/König (Hrsg.), *Kriminalsoziologie*, 3 (7 f.).

2248 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8), nennen ihr Szenario "Turning back the clock", wobei nicht ganz klar wird, zu welchem Zustand hier zurückgekehrt wird.

2249 So ist es auch bei hessenDATA schon der Fall gewesen, siehe HessLT-Drs. 19/6864 Teil B, S. 6 f.

se Persönlichkeitsrechte verletzt. Die nunmehr hegemoniale Position im sicherheitspolitischen Diskurs befürwortet eine stärkere Begrenzung von Massendatenüberwachung.<sup>2250</sup> Dabei ist die Kriminalitätsfurcht nicht homogen niedrig ausgeprägt. Zwar gibt es diejenigen, die von der relativen Sicherheit der Gesellschaft ausgehen oder eine höhere Unsicherheitstoleranz aufweisen. Daneben sind aber auch Einstellungen vorhanden, die sich durch eine relativ hohe Kriminalitätsfurcht und damit auch durch ein ausgeprägtes Unsicherheitsempfinden auszeichnen. Allerdings wird der Polizei und den mit ihr im Strafjustizsystem verknüpften Instanzen der staatlichen Sozialkontrolle einerseits eine wirksame Kriminalitätsbekämpfung nicht zugetraut und andererseits wird ein zu extensives polizeiliches Informationswesen klar als zum Unsicherheitsempfinden beitragender Faktor angesehen, sodass entsprechenden Ausweitungstendenzen mit politischer Ablehnung und Kritik begegnet wird. Bezüglich des Einsatzes überwachender und kontrollierende Informationstechnologie durch die Polizei ist im gesellschaftlichen Diskurs eine kritisch-dystopische sozio-technische Imagination eines hochtechnisierten polizeilichen Kontrollapparats hegemonial und entfaltet als mahnende Vision einer zu stark überwachten Gesellschaft hemmende Wirkungen auf informationstechnologische Innovationen. Affirmative Positionen, wie sie im Szenario 1 vorherrschend sind, haben kaum Diskursmacht.

## II. Technologische Entwicklung des Informationswesens

Die Technologisierung des polizeilichen Informationswesens hat massiv an Schwungkraft verloren und befindet sich an vielen Stellen in einer Sackgasse. Verglichen mit vergleichbaren Technologien des Privatsektors ist der technologische Standard der Polizei rückständig und gerät immer weiter ins Hintertreffen.

Ein zentrales Hindernis der informationstechnologischen Weiterentwicklung des polizeilichen Informationswesens ist die insofern blockierende rechtliche Struktur der Gesellschaft. Das liegt zum einen daran, dass grundrechtsinvasive Technologien vor ihrer Implementierung zunächst von unabhängigen Gutachter:innen eingehend geprüft werden müssen. Vor dem Einsatz müssen zudem noch umfassende Datenschutz-Folgenabschät-

---

<sup>2250</sup> Gerhold/Brandes Eur J Futures Res 9 (2021) (8).

zungen durchgeführt werden. Der Prozess ist langwierig und kostspielig, was insgesamt zu einer Verlangsamung des Innovationstempos führt.<sup>2251</sup> Diese Vorgaben für den Technologie-Einsatz in der polizeilichen Informationsverarbeitung erschwert die Entwicklung und Einführung von Massendatenverarbeitungsverfahren sowohl durch den Privatsektor als auch durch die Polizei selbst. Eine polizeiliche Sicherheitsindustrie kann sich nicht in Deutschland etablieren.<sup>2252</sup> Hinzu kommt eine für die Polizeien selbst schwer zu überschauende Regelungslage, die gepaart mit strengster Aufsicht durch die Landes- und Bundesdatenschutzbeauftragten den organisatorischen Ressourcenaufwand so gesteigert hat, dass nur sehr ausgewählte und dringende informationstechnologische Entwicklungsprojekte betrieben werden.

Zudem haben sich auch die träge Organisationsstruktur und bestimmte Organisationskulturen als wandlungsresistenter erwiesen, als einmal angenommen. Die Fachkulturen zwischen Polizeipraxis, Informationstechnologie und Verwaltung, wozu auch der interne Datenschutz zu zählen ist, sind mit den Komplexitäten der Integration von Polizeipraxis, technischer Infrastruktur und rechtlichen Vorgaben zunehmend überfordert und finden keine gemeinsame Sprache. Die haus eigene Entwicklung von neuen technischen Verfahren versandet häufig und auch der Einkauf von Software scheitert an organisatorischen Koordinations- und Integrationsproblemen, etwa weil Projekt-Spezifikationen nicht passen, sodass die technische Infrastruktur immer weiter veraltet und laufend Dysfunktionalitäten produziert. Informatiker:innen und sonstiges technisches Personal wandert zunehmend in die Privatwirtschaft ab. Aufgrund der Mängel des Informationswesens wird die Verwendung von technischen Verfahren von einer überwiegenden Mehrheit der operativ arbeitenden Polizist:innen abgelehnt. Ohnehin bestehen starke Widerstände gegenüber der Digitalisierung und Datafizierung der Polizeiarbeit, da ein Verlust der organisationsinternen Macht zugunsten der Führungsebenen befürchtet wird.<sup>2253</sup> Das „traditionelle Polizeihandwerk“ von Schutz- und Kriminalpolizei erfährt vor diesem Hintergrund eine Aufwertung gegenüber technisierten Formen der Polizeiarbeit.

---

2251 Gerhold/Brandes Eur J Futures Res 9 (2021) (8).

2252 Gerhold/Brandes Eur J Futures Res 9 (2021) (9).

2253 Siehe zu diesem Konflikt etwa Vera/Jablonowski in Stierle/Wehe/Siller (Hrsg.), Handbuch Polizeimanagement, 475; Reuss-Ianni, Two cultures of policing.

Das Projekt Polizei 2020 ist an der überbordenden Komplexität des heterogenen polizeilichen Informationswesens gescheitert. Es bestehen weiterhin Divergenzen zwischen den unterschiedlichen Länder- und Bundessystemen, Schnittstellen bleiben ein Problem. Datenübertragungen zu anderen Verwaltungszweigen sind ebenfalls nur bedingt möglich. Die informationstechnologische Infrastruktur erlaubt nur noch begrenzte Grundfunktionen wie den Datenaustausch, der aber – durch datenschutzrechtliche Vorgaben und technische Mängel bedingt – verlangsamt ist. Zudem übersteigt die Masse der Daten die Verarbeitungskapazitäten des Informationswesens und „verschmutzt“ die Datenspeicher. Datenabfragen produzieren nur noch begrenzt handlungsleitendes Wissen, da häufig zu viele widersprüchliche und falsche Daten in den Datenbanken abgelegt worden sind. Erkenntnisgewinnbringende Daten sind knapp. Daten sind, mit anderen Worten, zum Problem geworden.<sup>2254</sup> Einigen Länderpolizeien gelingt es besser als anderen die Funktionalitäten ihrer eigenen Systeme aufrechtzuerhalten, aber generell ist das polizeiliche Informationswesen immer weniger in der Lage, die zu seinem Erhalt und zu seinem Betrieb erforderlichen Aufwände durch entsprechende positive Effekte auf die polizeiliche Arbeit zu rechtfertigen.

Die technologische Diskrepanz der Polizei zu den übrigen Teilen der Gesellschaft produziert Folgeprobleme für die Polizei. Auf der einen Seite geraten die polizeilichen Systeme selbst immer wieder in den Fokus von Kriminellen, die mithilfe von technisch überlegenen Cyberangriffen sensible Daten aus den polizeilichen Datenbeständen zu Polizist:innen selbst, verdächtigen Personen, aber auch unter besonderem Polizeischutz stehenden Personen, wie hochrangigen Politiker:innen, erbeuten und diese schädigend nutzen: Betroffene werden mit der Veröffentlichung von persönlichen Daten erpresst, immer wieder kommt es zu Drohungen und weitergehenden Repressalien gegenüber denjenigen, deren Daten publik gemacht worden sind.<sup>2255</sup>

Vor allem macht sich die technologische Superiorität professionalisierter krimineller Felder aber darin bemerkbar, dass der polizeiliche Blick in bestimmten Kriminalitätsbereichen nur noch sehr oberflächlich Strukturen aufhellen kann. Vor allem in Bereichen, in denen es verfestigte Strukturen mit professionellen Täter:innen gibt, die ihre Kommunikations- und sonstige Technik stetig an fortschreitende Standards anpassen – also insbeson-

---

2254 Gugerli in Gugerli/Hagner/Hampe ua (Hrsg.), Nach Feierabend, 7 (7).

2255 Gerhold/Brandes Eur J Futures Res 9 (2021) (11 f.).

dere die organisierte Kriminalität, terroristische Täter:innen und Cyberkriminalität – gelingen der Polizei kaum noch Ermittlungserfolge. Terroristische Anschläge werden von der Sicherheitskultur mit einer gewissen „Gelassenheit“ (Münkler)<sup>2256</sup> hingenommen, lassen sich aber regelmäßig nur während ihrer situativen Entfaltung bekämpfen. Die organisierte Kriminalität agiert größtenteils von der rechtstreuen Gesellschaft unerkannt. Ab und an kommt es zu partiellen Aufdeckungen durch Medien oder seltene Ermittlungserfolge. Cyberkriminalität und Kriminalität, die in datenvermittelten Kontexten wie Umgebungen der sogenannten Smart City begangen wird, kann von der Polizei ebenfalls nur sehr begrenzt erkannt und dementsprechend kaum behandelt werden. Auch Kriminalität im Wirtschaftsleben, das hochtechnisiert und stark um Datenverarbeitungsprozesse herum organisiert ist, lässt sich kaum aufklären.

Polizeiliche Überwachungs- und Kontrolltätigkeiten sind in erster Linie auf die traditionellen (und analogen) Räume beschränkt. Die von der Polizei eingesetzte Informationstechnologie dient vor allem der Abkürzung von Arbeitsabläufen, etwa durch automatische Sprache-zu-Text-Umwandlung, oder zur Erleichterung der Kommunikation zwischen Beamt:innen im Einsatz. Es gibt allerdings kaum größere Integrationsverbünde von technischen Komponenten. Das polizeiliche Instrumentarium ist ansonsten auf hergebrachte „Werkzeuge“ wie Schusswaffen und sonstigen Verteidigungsmittel, Handschellen und einsatzunterstützende Hilfsmittel beschränkt.

### III. Polizeiliche Sozialkontrolle

Die vom Massendatenphänomen überforderte Polizei hat ihre einst zentrale Position im System der gesellschaftlichen Sozialkontrolle verloren. Damit geht ein genereller Bedeutungsverlust der staatlichen Sozialkontrolle in der zunehmend datafizierten Welt einher, da die Polizei als diejenige Institution wegfällt, die allen voran Devianz identifiziert und filtert.

Die beschriebenen Probleme der Wissensgenerierung der Polizei in der zunehmend digitalisierten Lebenswelt der Gesellschaft begrenzen den polizeilichen Wirkungsradius. Die Polizei ist primär im analogen öffentlichen Raum präsent und agiert dort als Produzentin sozialer Ordnung, etwa

---

2256 Münkler in Hucho/Nida-Rümelin/Julian, Sperling, Karl ua (Hrsg.), *Berichte und Abandlungen der Band Berlin-Brandenburgischen Akademie der Wissenschaften*, 101 (112).

im Kontext von gewalttätigen Auseinandersetzungen. Auch die kriminalpolizeiliche Tätigkeit ist im Wesentlichen auf die retrospektive Aufklärung klassischer Fälle beschränkt: Kapitaldelikte, Sexualstraftaten oder auch die abnehmenden Formen von Vermögensdelikten, die sich noch rein im analogen Raum begehen lassen. Polizeiarbeit findet also (wieder) vor allem auf „der Straße“ statt. Damit ergeben sich einerseits Potenziale für eine nahbare, gemeinschaftsbezogene Form der Polizeiarbeit (community policing<sup>2257</sup>).<sup>2258</sup> Gleichzeitig führt der Fokus auf „Straßenkriminalität“ jedoch weiterhin zu einer starken Überrepräsentierung von gesellschaftlichen Minderheiten und ohnehin bereits Ausgegrenzten im polizeilichen Fokus. Diese Selektivität hält Konfliktpotenzial für das Verhältnis zwischen Polizei und „Polizierten“ bereit. Dort, wo ein positives Verhältnis zur Gemeinschaft nicht hergestellt oder aufrechterhalten werden kann, kommt es zu Legitimationsverlusten, die Widerständen gegenüber den polizeilichen Einsatzkräften hervorrufen, worauf die Sicherheitspolitik mitunter mit einer – informationstechnologisch anspruchslosen – Militarisierung<sup>2259</sup> der Polizeitechnik reagiert.

Die Einschränkung des aufklärenden Blickes der Polizei führt auch dazu, dass sich Strukturen organisierter Kriminalität stärker ausbreiten und verfestigen können. Diese Strukturen fordern den staatlichen Ordnungsanspruch heraus und produzieren parallele Ordnungen in bestimmten Gebieten, in denen sie dann zwangsläufig auch (informelle) Sozialkontrolle an der Polizei bzw. des Staates statt ausüben.<sup>2260</sup> Damit ist keinesfalls eine nur fatalistisch rezipierbare Entwicklung eingeleitet, denn wie *Eisenstadt* bereits feststellte: „collapse, far from being an anomaly, both in the real world and in social evolutionary theory, presents in dramatic form not the end of social institutions, but almost always the beginning of new ones.”<sup>2261</sup> Insofern kommt es zu einer Pluralisierung der Akteure. So wird die bereits für die

---

2257 Corder in Reisig/Kane/Bradford (Hrsg.), *The Oxford handbook of police and policing*, 148.

2258 Gerhold/Brandes *Eur J Futures Res* 9 (2021) (9).

2259 Siehe zu diesem vorrangig aus dem US-amerikanischen Diskursraum stammenden Phänomen *Bieler PIJPSM* 39 (2016), 586; zur deutschen Situation siehe *Naplava* in Hunold/Ruch (Hrsg.), *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung*, 165.

2260 Siehe zu dieser Dynamik der Konkurrenz von Ordnungen und Regimen sozialer Kontrolle etwa *Timothy Raeymaekers*, *Collapse or Order? Questioning State Collapse in Africa*, Nr. 10, 2005, S. II f.

2261 *Eisenstadt* in Yoffee (Hrsg.), *The collapse of ancient states and civilizations*, 236 (243). Zwar ist der Kontext ein entwicklungsgeschichtlich anderer, aber diese

Spätmoderne beschriebene Privatisierung der Sozialkontrolle beispielsweise stark intensiviert.<sup>2262</sup> Mit der Verkümmernng staatlicher Sozialkontrolle und Ordnungsproduktion einher gehen Strategien der Responsibilisierung der Individuen für ihre persönliche Sicherheit und die Kommodifizierung der je eigenen Sicherheitsbedürfnisse.<sup>2263</sup> In der Folge kommt es zu einer räumlichen Multiplikation sozialer Ordnungen. In Städten etwa bilden sich in Vierteln mit besserem sozioökonomischem Status deutlich abgeschottete Gemeinschaften heraus. Die verschiedenen Formen und Grade sozialer Ordnungen bringen zudem stark abweichend ausgeprägte Subjektkulturen hervor. Diese verteilen sich sicherheitskulturell auf der eingangs beschriebenen Achse zwischen denjenigen, die gelassener mit Unsicherheit umgehen und denjenigen, die Unsicherheit als Bedrohung wahrnehmen, aber keinen produktiven Umgang damit finden. Mit der multipolaren Ordnungstopografie, in der die Polizei nur eine Ordnungsproduzentin von vielen ist, geht auch ein Wandel des gesamtgesellschaftlichen Normgefüges einher. Den Institutionen der staatlichen Sozialkontrolle gelingt es mit Trübung des polizeilichen Blicks immer weniger, eine minimale normative Integration der Gesellschaft zu leisten. In der Folge kommt es zu einer stärkeren Fragmentierung bzw. Pluralisierung der normativen Grundlagen der Gesellschaft.

#### *E. Drittes Szenario: Die Polizei als spezialisiertes Konfliktlösungsinstrument*

Die beiden vorstehenden Szenarien sind aus der Perspektive des grundgesetzlichen Wertefundaments der hiesigen Gesellschaft nicht erstrebenswert. Im Szenario der datenmächtigen Polizei ist es vor allem die faktische und umfassende Aushöhlung des Rechts auf informationelle Selbstbestimmung, die den normativen Leitvorstellungen des Grundgesetzes widerspricht. Die Möglichkeiten des polizeilichen Informationswesens auf Daten in der Gesellschaft zuzugreifen und darüber Wissen über Personen – etwa in Form von Persönlichkeitsbildern im Rahmen von Risikoprognosen – und Gruppen zu generieren sind unter den Aspekten der Streubreite und des Informationsgehalts von Daten, die bereits jetzt als dogmatische Kriterien zur

---

grundlegende Dynamik sozialer Evolution dürfte als einigermaßen universell gelten.

2262 *Shearing/Stenning* Social Problems 30 (1983), 493.

2263 Siehe dazu etwa *Singelstein/Kunz*, Kriminologie, S. 411 ff.



Bestimmung der Eingriffsintensität einzelner Maßnahmen dienen, kaum mit dem Verhältnismäßigkeitsgrundsatz in Einklang zu bringen. Auch das Szenario der überforderten Polizei kann nicht als vor dem Hintergrund des Grundgesetz erstrebenswerte gesellschaftliche Zukunft gelten. Ganz gleich, wie man sie konzeptualisiert – ob als Grundrecht auf Sicherheit<sup>2264</sup> oder als objektiv-rechtliche Schutzpflicht des Staates<sup>2265</sup> – ist die Sicherheitsgewährleistung eine dem Staat zentrale und ihn als verfasste Friedens- und Ordnungsmacht auch im Angesicht der Pluralisierung der Gesellschaft charakterisierende Aufgabe. Bestehen auch unterschiedliche Auffassungen darüber, wie die normativen Gehalte des Sicherheitsbegriffs auszugestalten sind und wie viel dann von der so oder anders verstandenen Sicherheit zu gewährleisten ist, so ist doch ein gewisses Maß an Sicherheit in Form einer fundamentalen sozialen Ordnung, die gleichsam die Gesellschaft bis zu einem gewissen Grad normativ zu integrieren vermag, eine anerkannte Grundvoraussetzung menschlicher Vergesellschaftung.

Vor diesem Hintergrund soll nun im Folgenden ein drittes Szenario entworfen werden, das einen vermittelnden Pfad zwischen den beiden wenig erstrebenswerten Zukünften der datenmächtigen bzw. überforderten Polizei aufzeigen möchte. Damit soll ein Beitrag zur Reflexion über die Bedeutung wachsenden Wissens und technologischer Beherrschung von sozialen Prozessen im Rahmen polizeilicher Sozialkontrolle für die heutige Gesellschaft geleistet werden. Ziel ist es dabei, den technologie-induzierten Risiken des polizeilichen Informationswesens mit regulativer Voraussicht zu begegnen und in Auseinandersetzung mit diesen Risiken eine produktive sozio-technische Imagination informationstechnisch fundierter Sozialkontrolle durch die Polizei zu entwickeln. Das folgende Szenario ist das der Polizei als ein spezialisiertes Konfliktlösungsinstrument der Gesellschaft.

---

2264 Isensee, Das Grundrecht auf Sicherheit.

2265 Siehe dazu etwa Aulehner, Polizeiliche Gefahren- und Informationsvorsorge, S. 431 ff; grundlegend zu Schutzpflichten Unruh, Zur Dogmatik der grundrechtlichen Schutzpflichten.

## I. Sicherheitskultur

Der Sicherheitsdiskurs ist – wie immer wieder gefordert – tatsächlich evidenzbasierter<sup>2266</sup> geworden, was eine prinzipiell rationale Sicherheitskultur in der breiten Bevölkerung befördert hat. Die Kriminalitätsfurcht ist einigermassen kongruent mit den jeweiligen Kriminalitätsrisiken der Betroffenen. Kriminalpolitischer Populismus vermag kaum mehr als überschaubare Teile der Wahlbevölkerung zu mobilisieren. Die Straf- und Sicherheitsgesetzgebung haben sich dementsprechend gewandelt. Legislative Projekte rezipieren in hohem Maße Erkenntnisse der kriminologischen Forschung, die als Fundament für kriminalpolitische Richtungsentscheidungen gelten. Dabei bedeutet eine rationale Sicherheitskultur hingegen nicht, dass es keine problematischen Kriminalitätsrisiken gibt. Vielmehr ist im sicherheitspolitischen Diskurs präsent, dass die globalisierte, digitalisierte und datafizierte Gesellschaft neue Phänomene sozialer Unordnung mit sich bringt, die einen stellenweise geänderten Überwachungs- und Kontrollmodus erforderlich machen. Die hochtechnisierte Gesellschaft hat vielfältige Vulnerabilitäten, etwa an den neuralgischen Punkten ihrer kritischen Infrastrukturen, in neuen virtuellen Räumen oder aufgrund ihrer grundsätzlich offenen Struktur. Tatsächlich bestehende Bedrohungen durch terroristische Täter:innen, Cyberkriminelle oder konkrete Formen nachgewiesener organisierter Kriminalität sind die neuen Schwerpunkte des Sicherheitsdiskurses und damit auch der Polizei.

## II. Technologische Entwicklung des polizeilichen Informationswesens

Die Entwicklung und der Einsatz von informationstechnologischen Verfahren zur Massendatenverarbeitung verlaufen innerhalb der polizeilichen Organisationen nach zwei getrennten und weitgehend entkoppelten Dynamiken.

Ein Teil der Polizei ist wieder vorrangig auf Streife im öffentlichen Raum. Die Polizeibeamt:innen sind mehrheitlich zu Fuß unterwegs und versuchen, ansprechbar zu sein und gleichzeitig Verbindungen zur örtlichen Gemeinschaft zu knüpfen, wodurch an ein traditionelles Modell der Polizeiarbeit angeknüpft wird. Diese Form der gemeinschaftsbezogenen

---

2266 Siehe zum Ideal der Evidenzbasiertheit aus jüngerer Zeit etwa B.-D. Meier *Kriminalpolitische Zeitschrift* 5 (2020), 1; M. Walsh *NK* 32 (2020), 24.

Polizeiarbeit wird durch die Einstellung von mehr Beamt:innen und die Investition in bessere Ausrüstung flankiert. Informationstechnologische Geräte und Verfahren werden zwar von der Polizei eingesetzt, dienen aber in erster Linie dazu, die Effizienz der internen Abläufe und der Kommunikation mit der Öffentlichkeit zu steigern.<sup>2267</sup> Zudem wurden die Beamt:innen hinsichtlich ihrer technischen Ausrüstung weniger letal ausgestattet. Nur sporadisch werden Schusswaffen getragen. Es werden deeskalierende Taktiken und möglichst wenig beeinträchtigende Angriffs- und Verteidigungstechniken gelehrt. Zudem sind die Polizeikräfte nur ein Akteur im System der Produktion und Gewährleistung sozialer Ordnung in der Öffentlichkeit. Neben den Streifenbeamt:innen existiert ein breiteres Tableau von Akteur:innen in Form von zivile Konfliktlösungsteams zu diesem Zweck. Die Polizeikräfte der gemeinschaftsbezogenen Polizei dienen in diesem pluralen System der Sicherheitsproduktion vor allem als Reserve für Situationen und Konflikte, die sich ohne eine institutionalisierte Zurschaustellung von staatlicher Macht und erforderlichenfalls auch durch die Anwendung von verhältnismäßiger Gewalt nicht lösen lassen. Dafür ist eine datenmäßige Erfassung von Sachverhalten nur sehr selten vonnöten. Intervenieren diese Polizeibeamt:innen und registrieren strafrechtlich relevantes Verhalten, werden die Daten auch nur begrenzt von der Polizei verarbeitet, sondern vor allem direkt an die anzulegende elektronische Strafakte der Staatsanwaltschaft übertragen, die so wieder stärker ihre Rolle als Herrin des Ermittlungsverfahrens im Bereich der herkömmlichen Kriminalität im öffentlichen Raum erlangt hat. Insgesamt ist der Grad des informationstechnologisch fundierten Überwachungs- und Kontrollpotenzials bei diesem Teil der Polizei eher gering. Eine vollständige oder auch nur möglichst umfassende polizeiliche Durchdringung des öffentlichen Raumes zum Zweck der sozialen Kontrolle ist allerdings auch nicht das Ziel dieser institutionell abgegrenzten gemeinschaftsbezogenen Polizeiorganisation.

Dem gegenüber steht der zweite, ebenfalls institutionell abgegrenzte Teil der Polizei, der auf die Aufklärung und Verfolgung bestimmter hochschädlicher Kriminalitätsfelder fokussiert ist. Dazu gehören vor allem die drei großen Kriminalitätsphänomene der globalisierten und digitalisierten Gesellschaft: Terrorismus, (tatsächlich bestehende<sup>2268</sup>) organisierte Krimina-

---

2267 Gerhold/Brandes Eur J Futures Res 9 (2021) (9).

2268 Für eine kritische Reflexion hinsichtlich des vom medial-politischen Diskurs mitunter etwas schnell verwendeten und nicht immer durch tatsächliche Erkenntnisse

lität und Cyberkriminalität. Es sind Formen der Devianz, die ohne staatliche bzw. polizeiliche Überwachung und Kontrolle das ihren schweren Formen innewohnende Schädigungspotenzial realisieren und gesellschaftliche Strukturen damit real und nachhaltig bedrohen können, sodass eine spezialisierte Bekämpfung dieser Straftaten durch eine spezialisierte Institution geboten ist. Auch bestimmte Formen der (organisierten) hochrangigen Wirtschaftskriminalität<sup>2269</sup> ließen sich dazu zählen. Dieser Teil der Polizei ist mithin ein spezialisiertes Instrument für die Bearbeitung originärer Unordnungsphänomene der spätmodernen Gesellschaft.<sup>2270</sup>

Dazu ist ein effektives, aber gleichsam beschränktes und darin kontrolliertes polizeiliches Informationswesen erforderlich. Hierfür haben diese spezialisierten Polizeikräfte ein breites informationstechnologisches Instrumentarium, das von invasiven und streubreiten Erhebungsmethoden über interoperable und gut strukturierte Datenspeicher bis hin zu leistungsstarken Datenanalyseverfahren reicht. Allerdings ist das darin liegende Überwachungs- und Kontrollpotenzial ständigen Einhegungsbemühungen unterworfen, die vom Recht initiiert sind. Neben materiellen Begrenzungen auf bestimmbar Personenkreise und konkretere Eingriffsschwellen auch im Vorfeld findet vor allem eine prozedurale Beschränkung des Informationswesens statt. Zur Kontrolle der polizeilichen Sozialkontrolle hat sich ein robustes und handlungsfähiges internes Datenschutzkontrollregime in den Polizeiorganisationen etabliert, das durch eine enge Aufsicht der Bundes- und Landesdatenschutzbeauftragten ergänzt wird. Das interne System zeichnet sich allerdings bereits durch eine hohe Überwachungs- und Kontrolldichte bezüglich der polizeilichen Datenverarbeitung aus, so dass die Aufsichtsbehörden regelmäßig keine akuten Missstände feststellen, sondern eher strategische Ausrichtungsentscheidungen des polizeilichen Überwachungs- und Kontrollapparats im sicherheitspolitischen Diskurs mitbeeinflussen. Gewährleistet wird dies zunächst durch eine präsente und starke Stellung der behördlichen Datenschutzbeauftragten. Da diese aber die massenhafte Erhebung und Verarbeitung der Daten nicht alleine auf ihre Rechtmäßigkeit überprüfen können, ist eine automatisierte techni-

---

fundierten Konzepts der organisierten Kriminalität siehe etwa Paoli/Vander Beken in Paoli (Hrsg.), *The Oxford handbook of organized crime*, 13.

2269 Liebl (Hrsg.), *Wirtschafts- und Organisierte Kriminalität*.

2270 Angelehnt an *Derin/Singelnstein*, *Die Polizei: Helfer, Gegner, Staatsgewalt*, S. 362, die ebenfalls für die Polizei als "abgesteckte Ausnahmebehörde mit wenigen spezifischen Kompetenzen" plädieren, die also ein Konfliktlösungsmechanismus unter vielen ist.

sche Datenschutzkontrollarchitektur implementiert worden, die aus zwei wesentlichen Elementen besteht: Einerseits ist ein umfassendes Protokollierungssystem geschaffen worden, das lückenlos jede Datenerhebung und daran anschließende Verarbeitung bis zur Löschung dokumentiert. Die dabei anfallenden Protokolldaten über das aggregierte Informationshandeln der Polizei werden algorithmengestützt und gleichfalls automatisiert nach Mustern durchsucht, die auf einen rechtswidrigen Datenumgang hindeuten, wonach Verdachtsfälle dann durch die behördlichen Datenschutzbeauftragten gesondert geprüft werden. Andererseits ist das polizeiliche Informationswesen bezüglich seiner Löschungsvorgaben, also hinsichtlich des Rechts auf Vergessen im polizeilichen Kontext, automatisiert. Daten werden also bei ihrer Erhebung anhand ihrer personenbezogenen Klassifikation einem automatisiertem Löschregime unterstellt, das nur in Ausnahmefällen nach Konsultation der behördlichen Datenschutzbeauftragten in wichtigen Ermittlungskomplexen suspendiert werden kann. Geschieht dies nicht, „vergisst“ das polizeiliche Informationswesen automatisiert nach entsprechend festgelegten Zeiträumen personenbezogene Daten unwiederbringlich, wodurch die polizeilichen Datenbestände laufend verjüngt werden.

Die Fokussierung dieses Teils der Polizei auf bestimmte Kriminalitätsfelder macht es zudem leichter, informationstechnologische Infrastrukturen und Verfahren zur Massendatenverarbeitung zu entwickeln und zu implementieren, da die informationellen Bedürfnisse, die miteinander harmonisiert werden müssen, nicht mehr so stark divergieren, wie in der vorherigen organisationalen Struktur. Gleichzeitig kann durch diese graduelle Senkung des Komplexitätsniveaus des polizeilichen Informationswesens ein größerer Fokus auf die Rechtmäßigkeitskontrolle von Technologie-Entwicklung und -einsatz gelegt werden. Es gibt genug zeitliche und sonstige Ressourcen, um eine Anpassung von Technologien an die Regulierungsstrukturen zu vollziehen, um Sicherheitslücken zu identifizieren und zu schließen und um die Polizeibeamt:innen im rechtmäßigen Umgang mit den technologischen Verfahren zu schulen.<sup>2271</sup> Damit aber diese datenmächtigen Polizeikräfte auch von möglichen Devianzphänomenen erfahren, die ihrem Zuständigkeitsbereich unterfallen, aber im Blickfeld der gemeinschaftsbezogenen Polizeikräfte auftauchen, bestehen eng umgrenzte Datenübermittlungspflichten anlässlich bestimmter Verdachts- oder Erkenntnismerkmale. Neben einem operativen Apparat für die Durchführung von polizeilichen

---

2271 Gerhold/Brandes Eur J Futures Res 9 (2021) (9).

Maßnahmen von Datenerhebungen bis zu Festnahmen besteht zudem eine grundsätzliche, wenn auch selten akute Notwendigkeit für die auf hochschädliche Kriminalitätsfelder spezialisierte Polizei einzugreifen, wenn sich etwa terroristische Risikopotenziale im öffentlichen Raum zu materialisieren drohen oder materialisiert haben. Dazu sind, wie schon heute, entsprechende Eingreifteams eingerichtet. Im Gegensatz zur gemeinschaftsbezogenen Polizei sind diese Beamt:innen durchgehend mit letalen Waffen ausgestattet und können je nach Einsatzszenario auch mit entsprechenden informationstechnologischen Instrumenten ausgestattet werden – etwa mit mobilen Videosysteme wie Bodycams zur biometrischen Identifizierung von Zielpersonen oder zur Erkennung verdächtigen Verhaltens sowie mit weiteren bereits oben nach *Bain et al.*<sup>2272</sup> beschriebenen Geräte und Verfahren.<sup>2273</sup>

### III. Polizeiliche Sozialkontrolle

Die polizeiliche Sozialkontrolle im Szenario der Polizei als spezialisiertes Konfliktlösungsinstrument lässt sich vor allem als modular beschreiben: Der Einfluss der gemeinschaftsbezogenen Polizei auf die Produktion sozialer Ordnung ist relativiert und von eher abnehmender Tendenz. Die Pluralisierung der Akteure zur Bearbeitung von verbreiteter und gewöhnlicher Devianz bzw. zur – effektiveren – Bearbeitung der damit verbundenen sozialen Missstände und Konflikte verdrängt die Polizei ein Stück weit aus diesen Feldern. Zwar ist auch die Polizei weiterhin an sozialer Kontrolle etwa im öffentlichen Raum beteiligt, aber hauptsächlich gewährleistet sie einen Rahmen, innerhalb dessen vielfältige Konfliktlösungsteams den Versuch eines sanfteren Umgangs mit Devianz unternehmen und durch ihren höheren Professionalisierungsgrad – beispielsweise im Bereich der Drogenprävention und -arbeit – auf eine nachhaltigere Adressierung von deviantem Verhalten zugrundeliegenden Konfliktpotenzialen hinarbeiten. Damit einher geht eine gewisse Akzeptanz spätmoderner Ordnungsphänomene, die in einer Welt des „eskalierenden Wandels“<sup>2274</sup> multiple Normgefüge nebeneinander hervorbringt. Im Gegensatz dazu versucht die auf

---

2272 Siehe zum Folgenden *Bain/Carson/Conser* ua in Bain (Hrsg.), *Law Enforcement and Technology*, 115 (126 ff.).

2273 Siehe dazu bereits oben S. 503 f.

2274 *Sheptycki* *Global Crime* 18 (2017), 286 (296).

hochschädliche Kriminalitätsfelder fokussierte Polizei über ihre begrenzte Datenmacht eine möglichst umfassende und – wegen immer nur begrenzt vorhandenen Ressourcen – selektive, also möglichst auf die „gefährlichsten“ Individuen und Strukturen gerichtete, Sozialkontrolle zu etablieren. Die informationelle Durchdringung bestimmter gesellschaftlicher Felder ermöglicht es den begrenzt datenmächtigen Polizeikräften zudem, neue Kriminalitätsphänomene zu identifizieren und darauf zu reagieren. Die Modularität der polizeilichen Sozialkontrolle bedeutet also auch eine Flexibilisierung der Ausrichtung des polizeilichen Fokus, womit auch bisher „underpoliced“ Bereiche wie etwa hochrangige Wirtschaftskriminalität erschlossen und polizeilicher Sozialkontrolle zugeführt werden können.<sup>2275</sup> Die Fragmentierung sozialer Ordnungen in der spätmodernen Gesellschaft bringt also eine zunehmend plurale, mehrbene und netzwerkartige Sozialkontrolle hervor, in der die Polizei – auf den niedrigeren Ebenen Netzwerke von pluralen Akteuren der Bearbeitung von Devianz unterstützt, während sie auf den höheren Ebenen zu einem spezialisierten Instrument der Ausübung durchgreifender Sozialkontrolle gegenüber hochschädlichen Kriminalitätsfeldern wird.<sup>2276</sup>

*F. Regulierung: Kollektive Handlungsfähigkeit gegenüber dem sozio-technischen Großsystem des polizeilichen Informationswesens*

Dem französischen Technikphilosophen *Ellul* wird manchmal vorgeworfen, er zeichne ein hoffnungsloses Bild einer von der Technik besessenen und letztlich gefesselten Gesellschaft. Gleichzeitig bietet sein Werk aber stets auch Anknüpfungspunkte, um einem deterministischen Verhältnis von Technologie und gesellschaftlicher Entwicklung zu entkommen:

„[I]f man – If each one of us – abdicates his responsibilities with regard to values; if each of us limits himself to leading a trivial existence in a technological civilization, with greater adaptation and increasing success as his sole objectives; if we do not even consider the possibility of making a stand against these determinants, then everything will happen as I have described it, and the determinants will be transformed into inevitabili-

2275 Ähnlich etwa *Brayne*, *Predict and surveil*, S. 144.

2276 So auch – aber mit kritischem beziehungsweise skeptischem Unterton – *Sheptycki* *Global Crime* 18 (2017), 286 (296).

ties. [...] We must not think of the problem in terms of a choice between being determined and being free. We must look at it dialectically, and say that man is indeed determined, but that it is open to him to overcome necessity, and that this act is freedom. Freedom is not static but dynamic; not a vested interest, but a prize continually to be won. The moment man stops and resigns himself, he becomes subject to determinism. He is most enslaved when he thinks he is comfortably settled in freedom.“<sup>2277</sup>

Wie also lässt sich eine (kollektive) gesellschaftliche Handlungsfähigkeit herstellen oder erhalten, um im stetigen Ringen um Freiheit im Angesicht zunehmender informationstechnologischer Überwachungs- und Kontrollmöglichkeiten nicht in einen genügsamen, aber unfreien Stillstand zu geraten? Diese Frage führt zunächst zurück zum Ausgangspunkt dieses Kapitels, zu den sozio-technischen Imaginationen. Als kollektiv geteilte, institutionell stabilisierte und öffentlich praktizierte Vorstellungen einer wünschenswerten Zukunft, die durch eine normativ bedingte Technologie-Entwicklung beeinflusst wird, ermöglichen es sozio-technische Imaginationen Anstrengungen gebündelt auf die Erreichung eines gemeinsamen Ziels auszurichten.<sup>2278</sup> Für die Frage, wie sich eine Imagination gegenüber anderen durchsetzen kann, eignet sich das bereits eingeführte Konzept der Sicherheitskultur als Antwortansatz. In ihrem Rahmen finden gesellschaftliche Aushandlungsprozesse statt, mit denen die verschiedenen Akteur:innen darüber entscheiden, was als Gefahr anzusehen ist und wie dieser Gefahr – etwa mit technischen Mitteln – begegnet werden muss.<sup>2279</sup> Insofern ist die hegemoniale Sicherheitskultur untrennbar mit dem Aufstieg und Fall bestimmter sozio-technischer Imaginationen im Kontext gesellschaftlicher Sicherheitsbedürfnisse verbunden.<sup>2280</sup>

Die genauen Verlaufspfade der gegenwärtigen Sicherheitskultur lassen sich nur errahnen, aber ihre derzeitigen Eigenschaften und Dynamiken enthalten durchaus Potenziale für die Realisierung eines der beiden unerwünschten Szenarien. Daase zufolge ließe sich bereits jetzt „zeigen, dass der Wandel der Sicherheitskultur nicht nur zu institutionellen Veränderun-

---

2277 Ellul, *The Technological Society*, xxix, xxxiii. Dieser Zusammenhang der beiden Fundstellen ist übernommen von Sacasas, *What Is To Be Done? — Fragments*, <https://theconvivalsociety.substack.com/p/what-is-to-be-done-fragments> (Stand: 01.10.2023).

2278 Gerhold/Brandes *Eur J Futures Res* 9 (2021) (3).

2279 Daase *Aus Politik und Zeitgeschichte* 2010, 9 (9).

2280 Gerhold/Brandes *Eur J Futures Res* 9 (2021) (4).



gen und rechtlichen Verwerfungen in der Sicherheitspolitik führt, sondern generell staatliche Sicherheitsorgane und internationale Sicherheitsinstitutionen zu überfordern beginnt.“<sup>2281</sup> Der mittlerweile von überall aus der Gesellschaft schallende Anspruch auf staatliche Sicherheitsgewährleistung provoziert einen reflexhaft gewordenen staatlichen Legitimierungsimpetus- und -zwang – Sicherheitsgewährleistung für all jene (mit gesellschaftlichem Einfluss) im staatlichen Herrschaftsbereich – und trifft gleichzeitig auf begrenzte staatliche Ressourcen zur Produktion und Aufrechterhaltung von Sicherheit.<sup>2282</sup> Bezogen auf die Polizei als zentrale Akteurin staatlicher Sozialkontrolle und Sicherheitsgewährleistung lässt sich insofern ein Spannungsfeld ausmachen. Im Rahmen dieser Spannung drängt eine Dynamik – Sicherheitsansprüche und staatliche Legitimierungsbedürfnisse – in Richtung der datenmächtigen Polizei, die hoch technologisiert möglichst umfassende Sicherheit gewährleisten soll. Dem entgegen wirkt paradoxerweise die stetige Übernahme neuer Sicherheitsaufgaben und -versprechen durch den Staat und damit auch durch die Polizei. Denn die zunehmende Inanspruchnahme der begrenzten polizeilichen Ressourcen produziert laufend Potenziale für eine im Wesentlichen überforderte Polizei.

Insofern erscheint eine Neutralisierung dieser dysfunktionalen Tendenzen geboten, die ihren Ausgangspunkt in einer sukzessiven Umstellung des der Sicherheitskultur zugrundeliegenden normativen Gefüges nehmen muss. Eine rationalere Sicherheitskultur würde es sodann ermöglichen, nachhaltige sozio-technische Imaginationen der gesellschaftlichen Verwendung von informationellen Überwachungs- und Kontrolltechnologien zu entwickeln, die eine grundgesetzadäquate Sozialordnung auch in der spät-modernen Gesellschaft und darüber hinaus gewährleisten kann. Im Kern einer solchen Sicherheitskultur sollte vor allem ein Verständnis für die unhintergehbare *conditio humana* stehen. Sacasas schreibt in diesem Zusammenhang:

I would add, too, that because many of the problems we face are functions of the human condition, we cannot solve them, exactly—we can just find better ways of abiding them. Indeed, it may be that some of the problems we face stem precisely from the temptation to relate to the

2281 Daase Aus Politik und Zeitgeschichte 2010, 9 (16).

2282 Daase Aus Politik und Zeitgeschichte 2010, 9 (9).

human condition as one would to a technical problem in need of an engineered solution.<sup>2283</sup>

So sind den auch die vielfältigen Probleme, die die Gesellschaft mit deviantem Verhalten erfährt, zumeist Ausdruck sozialer Missstände und menschlicher Fehlbarkeiten, für die eine technologische Lösung selten oder nur unter stetiger Erhöhung des Drucks auf die menschliche Natur Abhilfe schaffen kann. Diese Idee ist auch dem gegenwärtigen System staatlicher Sozialkontrolle und der Polizei natürlich nicht völlig fremd. Damit sie aber zu einem robusten Kern einer neuen Sicherheitskultur werden kann, scheint eine rechtliche Programmierung der Sicherheitskultur, die ohnehin in ihren Strukturen stark normativ geprägt ist, erstrebenswert. Nun lässt sich *die* Sicherheitskultur nicht einfach durch *das* Recht umgestalten. Aber die Zukunft des polizeilichen Informationswesens wird entscheidend von gesetzgeberischen und gerichtlichen Entscheidungen abhängen.<sup>2284</sup> Um einem ausufernden technischen Solutionismus<sup>2285</sup> im allgegenwärtigen gesellschaftlichen Streben nach Sicherheit entgegenzutreten, gibt es also regulative Möglichkeiten, die freilich nicht ohne Weiteres generell auf die gesellschaftliche Produktion von Sicherheit angewendet werden können, sondern bereichsspezifischer Anpassung bedürfen.

Ein solcher – für die Sicherheitsproduktion zentraler – Bereich ist das vorliegend behandelte polizeiliche Informationswesen. Auch hier ist die Beförderung einer neuen Sicherheitskultur durch normative Programmierung keine von zentraler Stelle aus zu leistende Möglichkeit. Das Recht ist vielmehr ein Aushandlungsort, an dem die mit den drei Szenarien verbundenen sozio-technischen Imaginationen darum kämpfen, normativ festgeschrieben zu werden. Um (in einem systemtheoretischen Sinne) Anschlussfähigkeit im Recht zu erzeugen, müssen die Imaginationen dafür in dogmatische Konzepte überführt werden, sodass sie vom Rechtssystem prozessiert werden können.<sup>2286</sup>

Bestrebungen, das dritte hier gezeichnete Szenario normativ abzusichern, scheinen insofern besonders aussichtsreich, als es in besonderer Weise am Verhältnismäßigkeitsgrundsatz orientiert ist, der die gesamte grundgesetzliche Ordnung und damit auch die Sicherheitsverfassung rahmt. Insofern

---

2283 Sacasas, What Is To Be Done? — Fragments, <https://theconvivialsociety.substack.com/p/what-is-to-be-done-fragments> (Stand: 01.10.2023).

2284 Gerhold/Brandes Eur J Futures Res 9 (2021) (17).

2285 Morozov, To save everything, click here.

2286 Luhmann, Das Recht der Gesellschaft, S. 275.

ist das Szenario für alle jene Akteur:innen erstrebenswert, die sich einer verhältnismäßigen polizeilichen Informationsverarbeitung verpflichtet fühlen. Zudem sind ein Großteil der informationellen Erhebungsbefugnisse der Polizei – zumindest *de iure* – in ihrer grundsätzlichen Struktur vor allem Ausdruck dieses für die Verfassungsordnung grundlegenden Prinzips. Die Dogmatik des polizeilichen Informationswesens ist jedoch nicht angemessen entwickelt, wie *Bäcker* zutreffend sowohl für die rechtliche Regulierung der infrastrukturellen Aspekte wie den einheitlichen Informationsbestand im Sinne des Polizei 2020-Projekts, als auch für die Ebene des praktischen Datenumgangs im Informationswesen in Form vieler (neuer) Formen der Datenanalyse feststellt.<sup>2287</sup> Für beide Säulen des Informationswesens entwickeln sich zunehmend dogmatische Ressourcen für eine angemessenere Regulierung. Hervorzuheben sind etwa *Bäckers* Überlegungen zur rechtlichen Strukturierung von sogenannten verfahrensexternen Datensammlungen bei der Polizei, die einen Großteil des polizeilichen Informationswesens ausmachen. Das nach verfahrensübergreifenden und verfahrensunabhängigen sowie verfahrensinternen und verfahrensvorbereitenden unterscheidende Konzept erlaubt eine verhältnismäßige Strukturierung und Verwendung von polizeilichen Datensammlungen und sollte daher expliziter gesetzgeberisch rezipiert werden.<sup>2288</sup> Auf der Ebene des Datenumgangs, die immer mehr durch den Einsatz von Anwendungen künstlicher Intelligenz geprägt wird, gibt es bereits seit einiger Zeit dogmatische Bemühungen, regulative Konzepte zu entwickeln.<sup>2289</sup> Die neuartigen Formen der Datenauswertung etwa im Kontext des bereits bestehenden Datenabgleichs oder der neuen Anwendungen zur automatisierten Datenanalyse harren jedoch noch ihrer befriedigenden Bearbeitung.<sup>2290</sup> Mit Blick auf die Geschwindigkeit informationstechnologischer Innovation muss die dogmatische Auseinandersetzung um passende Konzepte für das polizeiliche Informationswesen zudem mehr als herkömmliche Rechtsdogmatik als stetiger Prozess verstanden werden, in dem es keinen Endpunkt, son-

2287 Zum ersten Aspekt siehe *Bäcker*, A-Drs. 18(4)806 D, S. 2, zum zweiten Aspekt *Bäcker* in Hoffmann-Riem (Hrsg.), *Big Data - Regulative Herausforderungen*, 167 (169 ff.).

2288 Siehe dazu *Bäcker*, *Kriminalpräventionsrecht*, S. 494 ff.

2289 Grundlegend zur Regulierung etwa *Martini*, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz*; für ein spezifisches Verfahren im polizeilichen Bereich siehe etwa die Empfehlungen von *Sommerer*, *Personenbezogenes Predictive Policing*.

2290 *Golla* *Kriminologisches Journal* 52 (2020), 149 (156 ff.).

dern nur aktuell mehr oder weniger gut an den gegenwärtigen Entwicklungsstand adaptierte Konzepte geben kann. Insofern ist *Gollas* Plädoyer für ein lernfähiges Recht der polizeilichen Informationsverarbeitung, das technologische Wandlungsprozesse laufend beobachtet und den rechtlichen Rahmen bedarfsweise korrigiert, unumwunden beizupflichten.<sup>2291</sup>

Dafür müssen der dogmatischen Diskussion ausreichend Material und Gelegenheiten zum Lernen gegeben werden. Zudem ist essenziell, dass das Gelernte auch Anwendung finden kann und nicht bereits durch die faktische Fortentwicklung des polizeilichen Informationswesens überholt worden ist.

Neben von *Golla* befürworteten Evaluationspflichten, parlamentarischen Unterrichtungen, Auslaufklauseln und besonderen Begründungserfordernissen bezüglich einzelner technischer Verfahren<sup>2292</sup> erscheint es auf Grundlage der vorliegend dargestellten Dynamiken des polizeilichen Informationswesens zudem notwendig, dessen technischen und organisationalen Schranken rechtlich zu verstärken bzw. wo erforderlich auch neu zu schaffen, um den bedenklichen Tendenzen polizeilicher Informationsverarbeitung zu begegnen. Zu verhindern ist vor allem, dass sich das sozio-technische Großsystem des polizeilichen Informationswesens zu einem verselbstständigten, nicht mehr kontrollierbaren Ensemble für (polizeiliche) Sozialkontrolle entwickelt,<sup>2293</sup> das die Freiheitssphären gesellschaftlicher Felder schleichend aushöhlt.<sup>2294</sup> Auf eine kurze Formel gebracht geht es also in erster Linie um die Überwachung und Kontrolle eines technischen Überwachungs- und Kontrollsystems. Neben dem demokratischen und rechtsstaatlichen Wert einer darüber herstellbaren Transparenz des polizeilichen Informationswesens wäre damit zudem der dogmatischen

---

2291 Siehe dazu *Golla* Kriminologisches Journal 52 (2020), 149.

2292 *Golla* Kriminologisches Journal 52 (2020), 149 (160).

2293 Siehe zu diesem theoretischen Konzept der "control without control" bereits *Thacker*, Networks, Swarms, Multitudes (Part Two), <https://journals.uvic.ca/index.php/ctheory/article/view/14541/5388> (Stand: 01.10.2023): "The political fantasy that is a by-product of these contradiction is that of a "control without control," the best of both worlds: a totally distributed, self-organizing, flexible and robust model of group organization, that can be directed towards certain ends, that is able to mobilize in a particular way, and that is able to express purpose or intention on a global scale."

2294 Siehe dazu bereits oben S. 484 f.

Entwicklung gedient, die mit klarerem Blick passgenauere Normstrukturen entwickeln könnte.<sup>2295</sup>

## I. Überwachung des aggregierten Überwachungs- und Kontrollverhaltens der Polizei: Überwachungsbarometer

Wie bereits weiter oben angesprochen ist die individualrechtsschützende Struktur des Grundgesetzes im Kontext des Massendatenphänomens nicht unproblematisch.<sup>2296</sup> In diese Richtung wendet es auch *Cheney-Lippold*:

“Privacy as an atomizing, isolating phenomenon is a privacy not worth fighting for. Privacy as intersubjective, social, and associative is a privacy worth thinking through and resuscitating.”<sup>2297</sup>

Insofern kann sich eine Überwachung des polizeilichen Informationswesens nicht auf Einzelfälle beschränken, sondern muss eine globale Perspektive einnehmen, mit der die unterschiedlichen Ausprägungen polizeilicher Überwachung und Kontrolle möglichst in ihrer Aggregation in den Blick genommen werden können. Das gilt vor allem, weil das polizeiliche Informationswesen ständig evolviert, wodurch sich die Eingriffsintensität von Datenumgang und Datenbeständen laufend wandeln kann.<sup>2298</sup> Insofern sind die für die Polizeien zuständigen Gesetzgeber gehalten, das polizeiliche Informationswesen als technologische Struktur in seinen unterschiedlichen Ausprägungen auf potenziell neue grundrechtliche Gefährdungslagen hin zu überprüfen und entsprechend ihrer parlamentarischen Regelungspflichten neu zu justieren.<sup>2299</sup> Zudem können die Gesetzgeber natürlich auch über diese Minimalverpflichtung hinausgehen und die polizeiliche Datenverarbeitung aktiv sicherheitspolitisch gestalten. Dafür muss allerdings auch eine proaktivere Auseinandersetzung mit Zustand und Wandlungsprozessen des polizeilichen Informationswesens aus einer Globalper-

2295 Ähnlich *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 12.

2296 Siehe dazu bereits oben S. 358 ff.

2297 *Cheney-Lippold*, We are data, S. 244.

2298 *Golla* Kriminologisches Journal 52 (2020), 149 (151); *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 4.

2299 Diesen Grundsatz hat das Bundesverfassungsgericht in seiner ersten Kalkar-Entscheidung für das technische Sicherheitsrecht formuliert, vgl. BVerfGE 49, 89 (130) – Kalkar I.

spektive erfolgen. Die Gesetzgeber müssen, so *Golla*, „verstärkt Instrumente und Verfahren einsetzen, um ihre ‚Produkte‘ und ihre Anwendung kritisch zu überprüfen.“<sup>2300</sup> Insofern muss ein adäquates Transparenzniveau hinsichtlich polizeilicher Datenbestände und Datenumgangsformen geschaffen werden.

Um dies in dem vorliegend vorgeschlagenen Umfang zu ermöglichen, erscheint in erster Linie das bereits in seinen Grundzügen dargestellte,<sup>2301</sup> bisher beispiellose und vor allem ebenfalls globalperspektivisch strukturierte Überwachungsbarometer für Deutschland von *Poscher, Kilchling und Landerer* geeignet. Ziel dieses Instruments ist die verstetigte und periodische<sup>2302</sup> Darstellung der staatlichen Überwachungslast in ihren unterschiedlichen Erscheinungsformen. So soll aufgezeigt werden, „wo reale Schwerpunkte der Überwachung liegen und wie diese sich insgesamt entwickelt“, um etwa je nach Bundesland oder Datenverarbeitungsverfahren differenziert Aussagen über Überwachungsintensität zu ermöglichen.<sup>2303</sup> In seiner gegenwärtigen modellhaften Fassung ist das Instrument auf die wesentlichen staatlichen Zugriffsrechte auf private Datenbestände gerichtet, was auch proaktive Berichtspflichten von Seiten der privaten Bestandsinhaber einschließt.<sup>2304</sup>

Allerdings wird das polizeiliche Informationswesen, wie es vorliegend als Verschränkung von informationstechnologischen Infrastrukturen und polizeilichen Informationspraktiken dargestellt wurde, nur sehr begrenzt erfasst. Vorliegend wird vor diesem insoweit beschränkten Umfang des Überwachungsbarometers für eine Ausweitung auf polizeiliche Datenbestände und polizeiliche Datenumgangsformen plädiert. Anders als *Poscher et al.* wird nämlich davon ausgegangen, dass das polizeiliche Informationswesen durch sein zu erwartendes Anwachsen unter dem Eindruck des Massendatenphänomens zumindest partiell den Charakter einer Massendatensammlung und – hier stimmen auch *Poscher et al.* zu – (behördlichen)

---

2300 *Golla* Kriminologisches Journal 52 (2020), 149 (160).

2301 Siehe dazu bereits oben unter S. 172 ff.

2302 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 4.

2303 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 7.

2304 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 10.

Vorratsdatenspeicherung aufweisen kann.<sup>2305</sup> Zudem ist aus hier vertretener Perspektive vor allem die Koppelung der sich aus dem polizeilichen Informationswesen ergebenden Datenmacht an die Institution der Polizei, die einen regen internen Datenaustausch pflegt, besonders relevant im Kontext staatlicher Überwachung und Kontrolle. *Poscher et al.* erfassen zwar den maßnahmenbezogenen Umfang staatlicher Massendatenüberwachung in ihrer Breite, ermöglichen aber nur bedingt eine Abschätzung institutioneller Machtakkumulation im Kontext staatlicher Überwachung und Kontrolle. Hinzukommt, dass polizeiliche Datenmacht – anders als etwa die von Nachrichtendiensten – wegen der polizeilichen Exekutivbefugnisse und ihrer Bedeutung im System strafrechtlicher Sozialkontrolle besonders folgenreich für einen größeren Teil der Bevölkerung sein kann. Zu erfassen wären für das polizeiliche Informationswesen der Umfang und die Intensitätsgrade informationeller Durchdringung durch polizeiliche Datenbestände und Informationspraktiken. Eine umfassende Erfassung des polizeilichen Informationswesens nach diesen Parametern müsste sodann auch eine sektorale Aufschlüsselung – etwa nach einer bestimmten Datenumgangsform (automatisierte Datenanalyse, Datenabgleiche, et cetera) – ermöglichen, um für bestimmte Ausprägungen dieses sozio-technischen Großsystems empirisch fundierter Intensitätsgrade hinsichtlich polizeilicher Überwachung und Kontrolle festzustellen.<sup>2306</sup>

Voraussetzung für eine solche Erfassung des Informationswesens durch das Überwachungsbarometer wäre – neben der Dokumentation der von *Poscher et al.* in den Blick genommenen Überwachungsmaßnahmen – die Erfassung und Zusammenführung der Informationen über polizeiliche Datenbeständen und tatsächlich anfallende Datenumgänge. Da ein Großteil des polizeilichen Datenumgangs im Informationswesen als Eingriffe von geringer Intensität gelten dürfte, ließe sich eine Dokumentationspflicht nicht aus der Verfassung ableiten,<sup>2307</sup> sondern wäre Ausdruck einer gestaltenden Sicherheitspolitik. Allerdings werden Datenabrufe in den polizeilichen Informationssystemen ohnehin bereits protokolliert. Zudem werden durch die Digitalisierung der polizeilichen Informationspraktiken – etwa

2305 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 6.

2306 So *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, 13 für das Überwachungsbarometer insgesamt.

2307 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 6.

in Form der Verwendung von Smartphones zum Datenabgleich im Einsatz – immer mehr Formen des polizeilichen Datenumgangs datenmäßig abbildbar, sodass das polizeiliche Informationswesen zunehmend Anknüpfungspunkte für die Etablierung einer reflexiven Überwachungspraxis bietet, die sich sodann auch ins Überwachungsbarometer einspeisen ließen. Im Idealfall wäre eine – vor allem durch das polizeiinterne Datenschutzkontrollregime<sup>2308</sup> ermöglichte – Nachverfolgung der Verarbeitungshistorie eines Datums von der Erhebung bis zur Löschung möglich. Dies wäre indessen ein notwendiger Zwischenschritt, um die Überwachungslast durch das polizeiliche Informationswesen in abstrakteren Größenordnungen aggregiert darzustellen. So ließen sich etwa Aussagen darüber treffen, welcher Anteil der Bevölkerung datenförmig in den polizeilichen Datenbeständen zu einem bestimmten Zeitpunkt abgebildet ist. Denkbar wäre es auch, zu ermitteln, welches Datenvolumen und welche Datenqualität in bestimmten Bereichen zu einem bestimmten Zeitpunkt erreicht ist, was Rückschlüsse auf den Intensitätsgrad der informationellen Aufschlüsselung bestimmter Phänomenbereiche und Personencluster geben könnte. Dabei sollten die Daten so aggregiert werden, dass sie auch wieder auf bestimmte Regionen, Behörden oder Datenbestände und Datenumgangsformen heruntergebrochen werden können und so ein granulares Bild des polizeilichen Informationswesens ermöglichen können. Inwieweit in diesen Aggregationen persönliche Merkmale zu den betroffenen Personenkreisen und sonstige Informationen zu individuellen Umständen der Datenverarbeitung rekonstruierbar sein sollten, lässt sich hier nicht abschließend diskutieren. *Poscher et al.* halten dies aus forschungsökonomischen Gründen für zu aufwendig und aus datenschutzrechtlicher Perspektive für nicht wünschenswert.<sup>2309</sup> Allerdings würde man insoweit auch eine Möglichkeit verspielen, diskriminierende Tendenzen und Dynamiken im polizeilichen Informationswesen zu identifizieren, was zu einer gerechteren polizeilichen Sozialkontrolle und rationaleren Sicherheitskultur beitragen könnte.

Die Realisierung eines solchen Überwachungsbarometers ist – vor allem in seiner periodischen Verstetigung – mit Schwierigkeiten behaftet. Bereits der einem institutionalisierten Instrument notwendigerweise vorausgehende Forschungsaufwand ist immens und braucht dementsprechend eine institutionelle Absicherung, was neben finanziellen Ressourcen vor allem

---

2308 Dazu sogleich im Anschluss an diesen Abschnitt.

2309 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 15.



auch die Unterstützung der entsprechenden staatlichen Stellen erfordert.<sup>2310</sup> Diese Schwierigkeiten würden durch die vorliegend für sinnvoll gehaltene Ergänzung des Barometers in der soeben beschriebenen Weise noch einmal potenziert. Erschwert wird eine solche Ergänzung zudem durch die Heterogenität des Informationswesens, wobei allerdings das Polizei 2020-Projekt mit seinem Ziel der Homogenisierung polizeilicher Datenhaltung und -verarbeitung auch als Chance für ein erweitertes Überwachungsbarometer verstanden werden muss. Hinzu kommen zu erwartende Widerstände polizeilicher Interessenvertretungen, die sich gegen eine Überwachung der Polizei und einen „Generalverdacht“ gegenüber Polizist:innen wenden. Diese Schwierigkeiten werden aber durch den potenziellen Nutzen eines solchen, um die beschriebene Erfassung des polizeilichen Informationswesens erweiterten Instruments nach hier vertretener Ansicht deutlich ausgeglichen. Zusammen mit den Datengrundlagen zu Kriminalität, die bereits bestehen und stetig ausgebaut werden, könne ein Überwachungsbarometer, das evidenzbasiert Auskunft über die staatliche bzw. polizeiliche Überwachungs- und Kontrolltätigkeit gibt, zu einer rationaleren Sicherheitskultur im oben beschriebenen Sinne<sup>2311</sup> beitragen. Eine insofern empirisch fundierte Rechtspolitik könnte besser über die Sinnhaftigkeit bestimmter polizeilicher Datenverarbeitungsformen diskutieren. Zudem könnten sich – da eine zu intensive Überwachung in individueller<sup>2312</sup> wie kollektiver<sup>2313</sup> Hinsicht die grundgesetzliche Verfassungsidentität berührt – neue rechtliche Grenzen für den Ausbau des polizeilichen Informationswesens ergeben.<sup>2314</sup>

Vor diesem Hintergrund ließe sich trotz aller Schwierigkeiten und gegen zu erwartende Widerstände von einem der Verfassungsidentität wegen gebotenen Projekt sprechen. Mit dem Überwachungsbarometer unter Einschluss des polizeilichen Informationswesens könnte ein wichtiger Akzent für eine Neujustierung der Sicherheitskultur gesetzt werden, die sich nach wie vor insbesondere durch eine Intensivierung von informationstechnologisch fundierter Überwachung und Kontrolle auszeichnet. Um das Barometer als Instrument zu institutionalisieren wäre, auch eine rechtliche Absicherung geboten. Dazu müsste ein adäquates Transparenzniveau sicher-

2310 Poscher/Kilchling, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 8.

2311 Siehe dazu oben unter S. 520.

2312 BVerfGE 156, 63 (123) – Elektronische Aufenthaltsüberwachung.

2313 BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.

2314 Poscher/Kilchling/Landerer, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 7 f.

heitsbehördlicher Datenbestände und Datenumgangsformen gewährleistet werden. Für das polizeiliche Informationswesen bedeutet das insbesondere die Pflicht, grundlegende Informationen über ihre Datensammlungen in öffentlich zugänglicher Form zur Verfügung zu stellen, damit besser abgeschätzt werden kann, wie Datenbestände durch welche Datenumgangsformen in der Praxis genutzt werden.<sup>2315</sup> Daneben könnte die Integration des polizeilichen Informationswesens in das Überwachungsbarometer wie bereits angedeutet auf das polizeiinterne Datenschutzkontrollregime zurückgreifen, das zudem unabhängig von einem Überwachungsbarometer zu intensivieren ist.

## II. Ausbau des polizeiinternen Datenschutzkontrollregimes

Ob ein „umfassendes, polizeiliches Kontrollsystem“ in der Gesellschaft wahrscheinlich ist, kann vor dem Hintergrund der hohen technischen Komplexität des polizeilichen Informationswesens und seiner vielfältigen gegenläufigen Entwicklungsdynamiken bezweifelt werden.<sup>2316</sup> Nichtsdestotrotz zeigt die Nutzung der informationstechnologischen Möglichkeiten in anderen Ländern, dass die von der digitalen Gesellschaft produzierten „Kontrollüberschüsse“<sup>2317</sup> durchaus zur Etablierung invasiverer Überwachungs- und Kontrollpraktiken durch insbesondere staatliche Akteure genutzt werden können.<sup>2318</sup> Insofern muss eine Polizei, die tatbestandlich ein immer größeres Tableau an informationellen Befugnissen hat<sup>2319</sup> und deren technischen Möglichkeiten sich stetig fortentwickeln,<sup>2320</sup> hinsichtlich der von ihr ausgeübten Sozialkontrolle in besonderer Weise ihrerseits kontrolliert werden. Das gilt umso mehr, als dass neuere informationelle Pra-

---

2315 So schon (ohne Bezug zum Überwachungsbarometer) *Bäcker* in T. Dreier/V. Fischer/van Raay ua (Hrsg.), *Informationen der öffentlichen Hand - Zugang und Nutzung*, 229 (246 f.), der aber bereits fordert, dass die "erforderlichen Änderungen und Neuregelungen auf einem Gesamtkonzept beruhen [müssen], das die einzelnen transparenzgewährleistenden Regelungsbausteine zueinander ins Verhältnis setzt".

2316 *Heinrich*, *Innere Sicherheit und neue Informations- und Kommunikationstechnologien*, S. 381.

2317 *Baecker*, *Studien zur nächsten Gesellschaft*, S. 169; *Nassehi*, *Muster*, S. 43.

2318 Für die Nutzung der Informationstechnologie zu Überwachungs- und Kontrollzwecken in autoritären wie demokratischen Kontexten siehe bereits oben S. 17 f.

2319 Interview 8, Pos. 39.

2320 Interview 14, Pos. 44.

zen wie die automatisierte Anwendung zur Datenanalyse oder Formen des Predictive Policing sich regelmäßig durch eine gewisse technische Opazität auszeichnen. Um hier weiterhin eine Überprüfbarkeit von Ergebnissen dieser technischen Erkenntnisinstrumente sicherzustellen, ist eine Verstärkung der Verfahrenssicherungen notwendig, die im Wechselspiel mit der technologischen Entwicklung evolviere müssen. Im Sicherheitsdiskurs erfolgt die Entscheidung für die Einführung neuer Technologien häufig nach der Prämisse, dass alles, was technisch möglich ist, auch praktisch umgesetzt und rechtlich zugelassen werden sollte. Es scheint nur konsequent, dies nicht nur für technische Verfahren zu fordern, mit denen polizeiliche Sozialkontrolle effektiviert werden kann, sondern auch zur Verbesserung der Kontrolle der polizeilichen Sozialkontrolle. Das bereits zuvor beschriebene interne Datenschutzkontrollregime der Polizeien<sup>2321</sup> sollte also als rechtsstaatlich und demokratisch gebotene Erweiterung und Intensivierung der Kontrolle des polizeilichen Informationswesens begriffen und ausgebaut werden, um dessen Potenzialen für Missstände, Verselbstständigung und Dysfunktionalitäten etwas entgegenzusetzen. Für eine umfassende Kontrolle des polizeilichen Informationswesens erscheinen vor allem Strukturen relevant, die eine systematische und auf das aggregierte polizeiliche Informationshandeln in seiner Gesamtheit gerichtete Kontrolle ermöglichen. Damit soll individuellen Kontroll- und Rechtsschutzmöglichkeiten wie datenschutzrechtlichen Auskunftsrechten nicht ihre Zweckmäßigkeit abgesprochen werden. Aber eine umfassende Überwachung und Kontrolle der polizeilichen Informationsverarbeitung bezüglich ihrer Rechtmäßigkeit kann über eine solche sehr punktuelle Überprüfung, die zudem von der Geltendmachung durch individuelle Rechtsträger:innen abhängt, nicht gewährleistet werden. Um das kollektive Risikopotenzial von polizeilicher Datenverarbeitung zu adressieren und perspektivisch auch die Einbindung des polizeilichen Informationswesens in ein periodisches Überwachungsbarometer zu unterstützen, erscheint vor allem eine Intensivierung der Protokollierung polizeilichen Informationshandelns und die Stärkung der Position der Datenschutzbeauftragten geboten. Zudem sollte das Recht auf Vergessenwerden im Kontext polizeilicher Datensammlungen gesellschaftlich neu verhandelt werden.

Im Zentrum des polizeiinternen Datenschutzkontrollregimes muss die Protokollierung stehen. Schon jetzt sind in vielen polizeilichen Systemen

---

2321 Siehe dazu bereits oben S. 361 ff.

auch immer Verwaltungsdaten gespeichert, zu denen auch ID-Nummern, Speicher- und Änderungsdaten sowie Besitzdaten eines Datensatzes gehören. Damit ist es grundsätzlich möglich, „jede Änderung und Löschung, aber auch jede Einsicht mitsamt dem Anfrageanlass“ zu dokumentieren.<sup>2322</sup> Die Protokollierungspraktiken in den deutschen Polizeibehörden sind zurzeit nicht einheitlich.<sup>2323</sup> Idealerweise sollte – wo technisch möglich – jeder Datenumgang durch Polizist:innen so protokolliert werden, dass eine vollständige Rekonstruktion und Überprüfung des Umgangs erfolgen kann. In vielen polizeilichen Informationssystemen scheint dies – dem vorstehenden Zitat von *Kathke* nach – bereits zumindest technisch möglich zu sein. Zudem sollten neue Potenziale zur Protokollierung polizeilichen Informationshandelns – etwa in Form des Datenabgleiches im Einsatz über Smartphones und ähnliches – ebenfalls genutzt werden, um die Interaktionen von Beamt:innen mit dem polizeilichen Informationswesen möglichst zu dokumentieren und damit einer Kontrolle zugänglich zu machen.<sup>2324</sup> Dafür müssen jedoch auch ausreichende Ressourcen zur Verfügung gestellt werden.

Eine Kontrolle der so massenhaft anfallenden Protokolldaten lässt sich händisch auch auszugsweise kaum mehr bewerkstelligen, sodass auch hier über die Nutzung technischer Verfahren nachgedacht werden sollte. Die Verarbeitung von Massendaten mit dem Ziel über mustererkennende Algorithmen bestimmte Verhaltensformen zu identifizieren, lässt sich nicht nur auf abweichendes Verhalten in bestimmten Kriminalitätsfeldern, sondern theoretisch auch auf das aggregierte polizeiliche Informationshandeln anwenden. Insofern erscheint die Entwicklung von KI-gestützten Auswertungsverfahren zur Detektierung von rechtswidrigen oder in einem weiteren Sinne schädlichen Informationspraktiken im Informationswesen der Polizei denkbar. Damit könnten nicht nur missbräuchliche Informationspraktiken wie die immer wieder medial bekannt werdenden intentionalen Datenmissbräuche illuminiert werden.<sup>2325</sup> Vielmehr wäre damit auch die Möglichkeit einer laufenden systematischen Überprüfung eines Großteils polizeilicher Handlungen eröffnet, mit der Defizite und Fehlentwicklungen

---

2322 *Kathke*, Überlieferungsbildung aus, Fachverfahren Überlegungen zu POLAS BW der Polizei Baden-Württemberg, 2015, S. 16.

2323 Siehe dazu bereits oben S. 400.

2324 Siehe zur möglichen praktischen Umsetzung eines solchen Kontrollrahmens etwa *Fährmann* MultiMedia und Recht 24 (2021), 775 (778).

2325 Siehe dazu bereits Fn. 730.

gen identifiziert ausgeglichen werden könnten. Ein naheliegendes Anwendungsfeld wäre die Identifizierung von eventuell (unintentional) diskriminierenden Polizeipraktiken. Zumindest ließe sich ermitteln, in welchem Umfang und Verhältnis etwa Daten von Personen aus bestimmten sozio-ökonomischen Schichten vorhanden sind und verarbeitet werden. Mit der algorithmengestützten Überprüfung des eigenen Informationshandelns könnte die Polizei zudem versuchen, ihre blinden Flecken aufzuhellen und stereotype Wahrnehmung durch das Füllen von lückenhaften Datenbeständen zu korrigieren; das würde aber vor allem voraussetzen, dass Daten nicht nur aus denjenigen soziodemografischen Schichten erhoben werden, über die die Polizei ohnehin schon zahlreiche Datenpunkte besitzt, sondern auch dort, wo der polizeiliche Blick bisher nur oberflächlich schaut.<sup>2326</sup> Damit könnte ein wichtiger Schritt in Richtung einer polizeilichen Sozialkontrolle gegangen werden, die in der pluralen Gesellschaft der Spätmoderne mit ihren vielfältigen normativen Ordnungen weniger starke Verzerrungen – wie die überdurchschnittliche Erfassung von insbesondere ausländischen Minderheiten durch staatliche Sozialkontrolle – erzeugt.

Neben die Protokollierung sollte auch eine starke interne Kontrolle durch die behördlichen Datenschutzbeauftragten der Polizeien treten. Teilweise sind die Datenschutzbeauftragten schon in einer wirkmächtigen Position und können dem gesetzlichen Leitbild entsprechend beraten und vor allem auch recht frei kontrollieren. Allerdings scheint es durchaus auch Bedarf an einer (weiteren) Stärkung der Position beziehungsweise Aufstockung der zur Verfügung stehenden Ressourcen, etwa in Form von Personal zu geben, um eine adäquate Aufgabenerfüllung zu gewährleisten. Denn für eine dem gesetzlichen Leitbild entsprechende Beratung und Kontrolle ist ein umfassender Einblick in das polizeiliche Informationswesen in seinen spezifischen Ausformungen und Wirkweisen im jeweiligen Zuständigkeitsbereich vonnöten. Nur dann ist die erforderliche Einbindung in informationstechnologische Verfahren und Entwicklungsprozesse und damit eine optimale Nutzung von Beratungs- und Kontrollkapazitäten möglich. Vor allem auch die fortlaufende Entwicklung der Datenverarbeitungstechnologie gebietet eine stetige Anpassung der Handlungsmöglichkeiten der polizeilichen Datenschutzbeauftragten. Mit Blick auf die Fachkulturen der Technik, des Rechts und der Polizeifachlichkeit, die dem polizeilichen Informationswesen sein Gepräge geben, erscheint es zudem geboten, die dafür erforderliche Expertise im polizeiinternen Datenschutzkontrollregime

2326 In diese Richtung beispielsweise *Brayne, Predict and surveil*, S. 106.

entsprechend abzubilden, wobei hier sowohl die personelle Aufstockung, also die Einrichtung einer Datenschutzabteilung, als auch die personelle Weiterbildung, also die weitere Professionalisierung der einzelnen Datenschutzbeauftragten, als gangbare Wege erscheinen.

Die Polizei mag diese Forderungen nach engerer Überwachung und Kontrolle ihres informationellen Handelns durch Ausweitung der Protokollierung und Intensivierung der internen Überprüfung durch die behördlichen Datenschutzbeauftragten als Misstrauen wahrnehmen. Gerade über solche Überwachungs- und Kontrollmechanismen wird aber das in einem demokratischen Rechtsstaat so essenzielle Vertrauen in die staatliche Handlungsmacht überhaupt erst möglich. Vor diesem Hintergrund sollte auch der bisweilen von polizeilichen Interessensvertretungen kritisierte „Generalverdacht“, unter den man Polizei und Polizist:innen zu Unrecht gestellt sieht, in positivem Sinne umgedeutet werden. Anstatt das gesellschaftliche Verlangen nach einer rechenschaftspflichtigen Polizei abzuwerten, sollte das Stehen unter „Generalverdacht“ vielmehr Teil des polizeilichen Selbstverständnisses werden, denn: eine demokratische Polizei ist eine kontrollierte Polizei.<sup>2327</sup>

Ein letzter, aus hier vertretener Sicht zentraler Aspekt des internen Datenschutzkontrollregimes muss das Recht auf Vergessenwerden i.S.d. Art. 17 DS-GVO im Kontext des polizeilichen Informationswesens sein, in gesetzlichem Duktus häufig etwas weniger verfassungssprachlich als Lösungsverpflichtung und (dieser Verpflichtung vorgelagert) Aussonderungsprüffristen gefasst. Während die gesellschaftliche Medienentwicklung über Jahrtausende darauf bedacht war, das Erinnern und Aufbewahren von Informationen zu optimieren, dreht sich die Notwendigkeit von Vergessen und Erinnern im digitalen Zeitalter um.<sup>2328</sup> Mayer-Schönberger argumentiert, dass Vergessen in der massendatenbasierten Informationsgesellschaft nützlich und notwendig ist.<sup>2329</sup> Das gilt auch für das polizeiliche Informationswesen, dass als je nach Datenlage als mehr oder weniger detailliertes Kriminalitätsgedächtnis der Gesellschaft konzeptualisiert werden kann. Insofern müssen Strategien und Technologien des digitalen Vergessens für die polizeilichen Datenbestände entwickelt werden.<sup>2330</sup> Dabei müssen neben

---

2327 Derin/Singelnstein, Die Polizei: Helfer, Gegner, Staatsgewalt, S. 350.

2328 Mayer-Schönberger in Reiter/Wittmann-Tiwald (Hrsg.), Goodbye privacy - Grundrechte in der digitalen Welt, 9 (9).

2329 Mayer-Schönberger, Delete.

2330 Burkhardt, Digitale Datenbanken, S. 339.

der dem Massendatenphänomen inhärenten Problem eines nicht mehr zu bewältigenden Datenvolumens für die Polizei vor allem auch Erwägungen bezüglich einer zu intensiven Sozialkontrolle, wie sie etwa Ausdruck in *Popitz* These von der Präventivwirkung des Nichtwissens (man könnte vorliegend auch ergänzen: des Vergessens) gefunden haben, eine wesentliche Rolle für die Ausgestaltung von organisationalen Vergessensprozessen spielen. Denn die Digitalisierung von gesellschaftlichen Prozessen lässt immer mehr Datenströme entstehen, die durch die informationstechnologische Entwicklung der Polizeien erfasst werden können. Einmal ins polizeilichen Informationswesen aufgenommen, können lange Aussonderungsprüffristen (bei Straftäter:innen regelmäßig zehn Jahre, siehe etwa § 77 BKGa) und rechtlich abgesicherte Dynamiken wie die Mitziehautomatik<sup>2331</sup> sedimenthafte Datenakkumulationen entstehen lassen: In einer Gesellschaft, die soziale Prozesse zunehmend über digitale Daten erfasst und festhält, werden mit dieser rechtlich-technischen Struktur auf lange Sicht mehr neue Daten gesammelt und „erinnert“, als dass sie „vergessen“ werden. Der Entwicklungsstand von Technologien zur Datenhaltung und Datenauswertung wird dann letztlich darüber entscheiden, ob die Polizei diese Datenansammlung zur Effektivierung ihrer Sozialkontrolle nutzen können oder ob sie orientierungslos auf der dadurch bewirkten Datenflut umhertreiben wird. Eine Auseinandersetzung mit einem zweckmäßigen Verhältnis von Erinnern und Vergessen im Kontext polizeilicher Informationsverarbeitung erfordert sicherlich einerseits eine tiefergehende Auseinandersetzung mit gegenwärtigen Speicherpraktiken, die bisher eher selten und dann auch nur schlaglichtartig durch Tätigkeitsberichte von Bundes- oder Landesdatenschutzbeauftragten beleuchtet wurde. Hier wäre eine systematischere Durchdringung der polizeilichen Datenbestände geboten, wozu auch der beschriebene Ausbau des polizeiinternen Datenschutzkontrollregimes beitragen könnte. Andererseits ist aber auch ein gesellschaftlicher Aushandlungsprozess mit dem Recht auf Vergessenwerden im Rahmen des polizeilichen Informationswesens verbunden. Letztlich ist es eine demokratische Wertentscheidung, was kollektiv über abweichendes Verhalten erinnert und was vergessen werden soll. Die für eine Entscheidung anzustellende Abwägung ist keine leichte, denn die Funktionsfähigkeit des polizeilichen Informationswesens und damit der Polizei selbst liegt mit in der Waagschale. Insofern geht es um (berechtigte) Sicherheitsbedürfnisse

---

2331 Siehe dazu bereits oben S. 258 f.

der Gesellschaft. Gleichzeitig gebietet das Grundgesetz die Resozialisierung von Rechtsbrecher:innen,<sup>2332</sup> wozu auch ein Verblässen von Stigma und Vorwurf im kollektiven Gedächtnis gehören muss. Insofern lässt sich eine (annähernd) totale Sozialkontrolle durch die Polizei und weitere staatliche Akteure, die ein entsprechend umfassendes Erinnern als Grundvoraussetzung hat, nicht mit dem Grundgesetz vereinbaren. Die insoweit komplexen, multipolaren Abwägungsfragen werden sich nicht pauschal für *die* Kriminalität treffen lassen, sondern erfordern eine fortgesetzte und tiefgehende Auseinandersetzung mit dem polizeilichen Informationswesen und von ihm registrierten Devianzformen mitsamt ihrer Akteursfelder. Gerade diese Schwierigkeiten machen die Entscheidung über Vergessen oder Erinnern von abweichendem Verhalten aber zu einer zentralen und bisher ungelösten Herausforderung der spätmodernen Sicherheitskultur.

---

2332 Di Fabio in Dürig/Herzog/R. Scholz, Grundgesetz, Art. 2 Rn. 216 f.