EU-Datenschutz und Polizei

Die JI-Richtlinie im deutschen Polizeirecht

von Clemens Arzt[1]

Weitgehend unbeachtet neben der EU-Datenschutz-Grundverordnung landete die sogenannte JI-Richtlinie[2] auf den Tischen der Legislative und bedurfte der Umsetzung in nationales Recht. Die Bundesländer sind dabei sehr unterschiedliche Wege gegangen. Eine ambitionierte Neuausrichtung des in die Jahre gekommen Rechts der polizeilichen Datenverarbeitung ist dabei ausgeblieben.

Mit der JI-Richtlinie (JI-RL) wird erstmals die rein innerstaatliche Datenverarbeitung durch Polizei und Strafjustiz direkt von europarechtlichen Vorgaben berührt. Frühere Regelungen betrafen allein den Datenaustausch zwischen den Mitgliedstaaten. Die JI-Richtlinie ist Teil der Novelle des EU-Datenschutzrechtes und steht gleichsam als „kleine Schwester"[3] neben der allseits bekannten Datenschutz-Grundverordnung (DSGVO). Bis zum 6. Mai 2018 sollte die Richtlinie in nationales Recht umgesetzt werden. In Deutschland haben sowohl Bund als auch Länder diese Frist überschritten, obgleich die Notwendigkeit seit April 2016 bekannt war.

Nach Art. 1 Abs. 1 enthält die JI-Richtlinie „Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für

1 Eric Töpfer sei hiermit ausdrücklich für die deutliche Kürzung und Überarbeitung meines Beitrages gedankt.

2 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates: Amtsblatt der Europäischen Union (Abl. EU) L 119 v. 4.5.2016, S. 89

3 Schwichtenberg, S.: Die „kleine Schwester" der DSGVO. Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz, in: Datenschutz und Datensicherheit 2016, H. 9, S. 605-609

die öffentliche Sicherheit." Nach Art. 2 Abs. 1 JI-RL gilt diese „für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken". Dies bedeutet, jenseits dieser Zwecke gilt unmittelbar die DSGVO, auch für die Polizei. Dies ist z. B. der Fall, wenn diese zum Schutz privater Rechte tätig wird, aber unter Umständen auch bei der Amts- oder Vollzugshilfe oder in Bereichen der Gefahrenabwehr, die nicht auf die Abwehr oder Verhütung einer möglichen Verletzung von Verbotsnormen im Straf- oder Ordnungswidrigkeitenrecht abzielen. Diese Anwendungsfelder der DSGVO sind im Einzelfall zu ermitteln und die Abgrenzung ist durchaus schwierig, wie etwa im Fall der Verarbeitung von Fingerabdrücken Asylsuchender nach § 16 Abs. 3 Asylgesetz durch das Bundeskriminalamt.

Die DSGVO und die JI-Richtlinie weisen eine hohe inhaltliche Übereinstimmung im Aufbau wie auch den rechtlichen Regelungen auf. Dabei kommt der DSGVO im Zweifelsfall ein inhaltlicher „Führungsanspruch" zu. Dass die Richtlinie gleichwohl deutliche Abweichungen von der DSGVO beinhaltet, dürfte vor allem dem politischen Willen geschuldet sein, die Polizeien der Mitgliedstaaten nicht umfassend den vergleichsweise hohen Standards der DSGVO zu unterwerfen. Diese Absicht setzt sich eindeutig fort in ihrer Umsetzung im deutschen Recht.

Anpassungsbedarf aus Sicht der Datenschutzaufsicht

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hatte im Oktober 2016 ein Positionspapier mit 33 Empfehlungen zur nationalen Umsetzung der JI-Richtlinie erarbeitet: So sei etwa zu vermeiden, dass Betroffenenrechte gegenüber der bisherigen Rechtslage etwa durch Begründungspflichten oder obligatorische Identitätsnachweise bei Auskunftsersuchen verkürzt werden. Die Anforderungen an den Nachweis einer ordnungsgemäßen Datenverarbeitung durch Polizei- und Justizbehörden sollten präzisiert werden, u.a. durch klare gesetzliche Anforderungen an technische und organisatorische Maßnahmen, weil effektiver Datenschutz gerade im Bereich der polizeilichen Datenverarbeitung nicht allein mit gesetzlichen Regelungen durchgesetzt werden könne. Entscheidungen der Polizeibehörden, Datenschutzverletzungen nicht zu melden, müssten für die Aufsichtsbehörden kontrollierbar und nachvollziehbar sein. Für Datenübermittlungen an Drittstaaten solle zum Zweck einer effektiven Kontrolle eine zentrale Protokollierung (vgl. Art. 25 JI-RL) mit ausreichenden Mindestfristen für die Speicherung

der Protokolldaten gesetzlich vorgeschrieben werden. Untersuchungs-, Anordnungs- und Klagebefugnisse der Datenschutzaufsichtsbehörden sollten bei der Umsetzung der JI-RL weitgehend übereinstimmend mit denen nach der DSGVO geregelt werden.[4]

Transformation der JI-Richtlinie durch „copy & paste"

Der Bund hat bei der Umsetzung der JI-RL für die Strafprozessordnung den Weg einer teilweisen direkten Implementation gewählt[5] und verweist im Übrigen auf eine entsprechende Anwendung der §§ 45 bis 84 des Bundesdatenschutzgesetzes (BDSG), welche Bestimmungen für Verarbeitungen zu Zwecken gemäß der JI-Richtlinie beinhalten. Dieses Regelungsmodell gilt auch für das Bundeskriminalamtgesetz. Für das Bundespolizeigesetz ist eine Novelle in der 19. Legislaturperiode im Bundesrat gescheitert.[6] Damit ist der Bund mit der Umsetzung bis zur Vorlage eines neuen Novellierungsvorschlages und einer Umsetzung dann vermutlich vier bis fünf Jahre im Verzug.

Die Umsetzung in den einzelnen Bundesländern kann hier aus Platzgründen nicht im Detail nachvollzogen werden. Der sächsische Gesetzgeber etwa hat sich dazu entschlossen, das Recht der (vollzugs-)polizeilichen Datenverarbeitung in zwei getrennten Gesetzen – dem Sächsischen Datenschutz-Umsetzungsgesetz (SächsDSUG) und dem Sächsischen Polizeivollzugsdienstgesetz (SächsPVDG) – zu regeln. Dagegen hat sich der Gesetzgeber in Mecklenburg-Vorpommern dezidiert für eine bereichsspezifische Anpassung der datenschutzrechtlichen Bestimmungen im Sicherheits- und Ordnungsgesetz des Landes entschieden hat.[7] In Berlin wurden die datenschutzrechtlichen Regelungen im Allgemeinen Sicherheits- und Ordnungsgesetz (ASOG) im Zuge der Novelle 2021 nicht einmal „angefasst". So verweist das ASOG beispielsweise weiter auf eine Fassung des Berliner Datenschutzgesetzes (BlnDSG), die seit langem außer Kraft ist. Bei der Novelle des BlnDSG hat der Gesetzgeber – wie die meisten anderen Bundesländer – die JI-Richtlinie soweit irgend möglich wortwörtlich

4 https://lfd.niedersachsen.de/startseite/datenschutzreform/richtlinie_justiz_inneres_ji_richtlinie

5 Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 v. 20.11.2019: Bundesgesetzblatt (BGBl.) I 2019, S. 1724

6 näher hierzu Arzt, C.: Bundespolizeigesetz – Wie weiter in der nächsten Legislatur? in: Zeitschrift für Rechtspolitik 2021, H. 7. S. 205-208

7 Landtag Mecklenburg-Vorpommern: LT-Drs. 7/3694 v. 5.6.2019

übernommen. Dabei bedient sich die JI-Richtlinie zum Teil gänzlicher anderer Begrifflichkeiten als das deutsche Polizeirecht. Deutlicher konnten die betroffenen Länder kaum demonstrieren, dass an einer aktiven Umsetzung auch der Intentionen des europäischen Datenschutzrechts kein Interesse bestand.

Die Umsetzung der JI-Richtlinie durch eine Trennung von Polizeigesetzen und dem allgemeinen Datenschutzrecht ist mit Blick auf die ohnehin schon komplexen Regelungen im Recht der polizeilichen Datenverarbeitung sowohl für Polizeivollzugsbeamt*innen als auch für Betroffene polizeilicher Maßnahmen von Nachteil. Zur Beurteilung der Rechtmäßigkeit einer Maßnahme im Bereich der Gefahrenabwehr sind nunmehr zwei getrennte Gesetze bei „klassischen" polizeilichen Tätigkeiten heranzuziehen. Bei einer nicht der JI-Richtlinie unterfallenden polizeilichen Verarbeitung personenbezogener Daten, also etwa beim Schutz privater Rechte, ist dann neben dem Polizeirecht auch noch die DSGVO zu konsultieren, um die rechtlichen Voraussetzungen der Datenverarbeitung bestimmen zu können. Nachfolgend sollen hier exemplarisch einige Umsetzungsprobleme am Beispiel Sachsen dargestellt werden.[8]

Polizeiliche Datenverarbeitung nach „Treu und Glauben"

In Sachsen hat der Gesetzgeber das Datenschutzrecht für die Polizei durch eine (nahezu) wörtliche Übernahme der JI-Richtlinie oder der §§ 45 ff. BDSG in ein eigenes Gesetz allein für die Datenverarbeitung durch die Polizei (SächsDSUG) übernommen. Damit scheint die Sache einfach und unangreifbar, verfehlt aber im Ergebnis das Ziel einer Einpassung in die Systematik des deutschen Polizeirechts[9] einerseits, insbesondere aber einen materiell-rechtlichen Ansatz bestmöglichen Schutzes des Grundrechts auf informationelle Selbstbestimmung andererseits. Ein Beispiel: Nach § 3 Abs. 2 Nr. 1 SächsDSUG sind personenbezogene Daten nach „Treu und Glauben" durch die Polizei (!) zu verarbeiten. Soll hier ein anderer, weiterer Maßstab neben der „Rechtmäßigkeit" im Sinne des Art. 4 Abs. 1 lit. a JI-RL und der Gesetzmäßigkeit und Gesetzesgebundenheit der Verwaltung wie auch dem Grundsatz der Verhältnismäßigkeit im

8 vgl. zu den folgenden Ausführungen: Arzt, C.: Umsetzung des europäischen Datenschutzrechts in Sachsen – SächsPVDG und SächsDSUG: eine kritische Bestandsaufnahme, in: Sächsische Verwaltungsblätter 2016, H. 12, S. 345-352

9 vgl. Aden, H.: Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BT-Ausschussdrucksache 18(4)824 G v. 27.3.2017, S. 5

Sinne des deutschen Rechts eingeführt werden oder dominierte hier einfach die Angst vor einer Rüge mangelhafter Umsetzung?

Verarbeitung besonderer Kategorien von Daten

Nach § 4 Abs. 1 Nr. 1 SächsDSUG ist jede „Verarbeitung" und damit auch die Erhebung besonderer Kategorien personenbezogener Daten i. S. v. § 2 Nr. 15 des Gesetzes nur zulässig, wenn diese unbedingt erforderlich und „in einer Rechtsvorschrift vorgesehen ist". Bei jeder Verarbeitung solcher Daten handelt es sich um einen schwerwiegenden Eingriff in die Grundrechte.[10] Entsprechende Eingriffsbefugnisse sollen ausweislich der Gesetzesbegründung im Fachrecht erfolgen. Sucht man indes im SächsPVDG nach spezifischen Erhebungs- oder Speicherungsregelungen für alltägliche polizeiliche Maßnahmen, wie etwa Speicherungen zur Zuordnung von Personen zu einem bestimmten politischen Spektrum, der ethnischen Herkunft oder zu HIV- oder anderen Infektionskrankheiten, so ist nicht erkennbar, wo das Polizeirecht solche Speicherungen ausdrücklich und begrenzend regeln würde.

Nach § 4 Abs. 2 Satz 1 sind bei der Verarbeitung besonderer Kategorien personenbezogener Daten geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Satz 2 legt diese indes nicht verbindlich fest, sondern beinhaltet nur unverbindliche Schutzoptionen. „Die konkrete Anforderung der Maßnahmen kann also von Einzelfall zu Einzelfall variieren",[11] ohne dass das Gesetz hier verbindliche Maßgaben festlegte.

Betroffenenrechte

Abschnitt 3 des SächsDSUG regelt die Rechte der von der polizeilichen Datenverarbeitung betroffenen Personen. § 12 regelt die Benachrichtigung, soweit im SächsPVDG eine solche vorgeschrieben ist, was insbesondere bei verdeckten Maßnahmen der Regelfall ist. Allerdings ist nicht für alle Datenverarbeitungen, die ohne Wissen des Betroffenen durchgeführt werden, eine Benachrichtigungspflicht vorgesehen. So ist es beispielsweise gängige Polizeipraxis, bei einer Identitätsfeststellung zugleich einen Datenabgleich durchzuführen, ohne dass der Betroffene hiervon

10 Johannes, P.C.; Weinhold, R.: Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze, Baden-Baden 2018, § 1 Rn. 143

11 Sächsischer Landtag: LT-Drs. 6/14791 v. 18.9.2018, S. 255

verpflichtend Kenntnis erlangte oder informiert würde. Gravierender noch ist aber die fehlende Benachrichtigungspflicht bei jedweder Speicherung und weiteren Verarbeitung in Datensammlungen der Polizei,[12] gerade in Zeiten zunehmender proaktiver Nutzung von Datenbeständen durch die Polizei.[13]

§ 13 Abs. 1 SächsDSUG gibt jeder Person ein Auskunftsrecht, ob die Polizei personenbezogene Daten über sie verarbeitet. Der Antrag ist voraussetzungslos. Verarbeitet die Polizei keine Daten zu der anfragenden Person, hat sie eine Negativauskunft zu erteilen. Anders als in Art. 15 Abs. 1 lit. h DSGVO vorgesehen, kennt die JI-Richtlinie jedoch kein Auskunftsrecht zu „aussagekräftige(n) Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Diese klare Lücke im Schutz von Betroffenenrechten wollte auch der sächsische Gesetzgeber nicht schließen.

Auch das pauschale Erfordernis einer Zustimmung von Geheimdiensten bei Auskunftsersuchen zu Übermittlungen an ebendiese in § 13 Abs. 3 SächsDSUG beschränkt die Betroffenenrechte über Gebühr. Art. 13 Abs. 3 JI-RL lässt eine Beschränkung des Auskunftsrechts nur soweit und solange zu, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist, allerdings nur sofern den Grundrechten und den berechtigten Interessen der betroffenen Person dabei Rechnung getragen wird.[14]

Datenschutz-Folgenabschätzung

In Umsetzung von Art. 27 JI-RL wie auch Art. 35 DSGVO verankert § 23 SächsDSUG „insbesondere bei Verwendung neuer Technologien" eine Pflicht zur Datenschutz-Folgenabschätzung. Angelehnt an § 67 BDSG hat der Gesetzgeber hier erhebliche Abweichungen von der JI-RL in das Gesetz eingefügt. Der dort verwandte Begriff des „hohen Risikos" wurde

12 Hierzu ausführlich Arzt, C; Müller, M.W.; Schwabenbauer, T.: Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in: Bäcker, M; Denninger, E.; Graulich, K; Lisken, H. (Hg.): Handbuch des Polizeirechts, München 2021, Kapitel G (Rn. 1108ff.)

13 Bäcker, M.: Normenkontrollantrag gegen das SächsPDVG v. 1.8.2019, S. 75 f., www.gruene-fraktion-sachsen.de/fileadmin/user_upload/ua/201908-Normenkontrollklage-Polizeigesetz.pdf

14 Schwichtenberg, S.: § 56 BDSG, in: Kühling, J.; Buchner, B. (Hg.): Kommentar Datenschutz-Grundverordnung BDSG Kommentar, München 2018, S. 1781 (Rn. 9)

durch den der „erhebliche(n) Gefahr“ ersetzt. Zudem wurde die europarechtliche Dimension einer Beurteilung anhand der „Rechte und Freiheiten natürlicher Personen“ durch „Rechtsgüter betroffener Personen“ ersetzt. Hier handelt es sich mitnichten um eine synonyme Ausdrucksweise.[15] Die deutliche Begrenzung der Pflicht zur Folgenabschätzung war offenbar Absicht des Gesetzgebers. Dies gilt auch für die Begrenzung auf „neue Technologien“. Diese ist zwar richtlinienkonform, wird indes besonders umstrittene, aber bereits genutzte Maßnahmen wie Quellen-TKÜ und Online-Durchsuchung ebenso ausschließen, wie Bodycams und die automatisierte Gesichtserkennung. Ob für diese Technologien jemals Datenschutz-Folgenabschätzungen durchgeführt werden, ist mit Blick auf die gesetzlichen Voraussetzungen mehr als zweifelhaft.

Datenschutzfreundliche Technikgestaltung

In Umsetzung von Art. 20 JI-RL hat Sachsen in § 27 SächsDSUG im Wesentlichen den Normtext des § 71 BDSG übernommen. Die Regelung zielt ab auf die Einhaltung der Grundsätze von „data protection by design and by default“. In der Gesetzesbegründung wird der Anspruch hieran sogleich auf einen „effizienten Mitteleinsatz in angemessenem Verhältnis zum angestrebten Schutzzweck“ eingegrenzt,[16] statt konkrete Schritte vorzugeben, welche Anforderungen die Polizei, die ja nicht Hersteller der von ihr eingesetzten vielfältigen Überwachungstechnologien ist, bei deren Erwerb und Einsatz stellen soll.[17]

Die enge Beschränkung des vom Gesetzgeber verfolgten Ansatzes findet ihren Ausdruck auch darin, dass § 27 Abs. 1 SächsDSUG – anders als Art. 20 Abs. 1 JI-RL – lediglich „Vorkehrungen“ statt technische und organisatorische Maßnahmen nennt.[18] Eine weitere Einengung findet statt, wenn als angemessene Vorkehrung zur Einhaltung von Datenschutzgrundsätzen wie Datensparsamkeit allein die Pseudonymisierung genannt wird, anstelle von Maßnahmen, die eine Erhebung personenbezogener

15 Hansen, M.: § 67 BDSG, in: Wolff, H.A.; Brink, S.: Beck‘scher Online Kommentar Datenschutzrecht, 37. Edition, München 2021, Rn. 8

16 Sächsischer Landtag: LT-Drs. 6/14791 v. 18.9.2018, S. 263

17 vgl. Marnau N.: § 71 BDSG, in: Gola, P.; Heckmann, D. (Hg.): Bundesdatenschutzgesetz Kommentar, 13. Auflage, München 2019, S. 694-703

18 ebd., Rn. 13

Daten möglichst von Anfang an vermeiden oder deren schnelle Löschung vorsehen.

Der Hinweis in der Gesetzesbegründung, dass keine Daten ohne menschliches Zutun erhoben und verarbeitet werden sollten,[19] übergeht den Grundansatz der datenschutzfreundlichen Voreinstellung, etwa mit Blick auf stark technikgetriebene Überwachungsmaßnahmen wie die automatisierte Gesichtserkennung oder den Kennzeichenabgleich nach §§ 58 und 59 SächsPVDG und die hierbei erhobenen Daten, die im Sinne der Datensparsamkeit zu beschränken sind.[20] Der Wille des Gesetzgebers, die Polizei durch konkrete Vorgaben in den Erhebungs- und Verarbeitungsregelungen im SächsPVDG auf eine aktive Beachtung der Grundsätze in § 27 zu verpflichten, zu denen auch der Grundsatz der Datensparsamkeit gehört, scheint hier deutlich entwicklungsfähig.

Datenschutzaufsicht

Anforderungen an die Befugnisse der Aufsichtsbehörde regelt Art. 47 JI-RL, der durch § 40 SächsDSUG umgesetzt werden soll. Nach der JI-RL müssen die Mitgliedsstaaten durch Rechtsvorschriften vorsehen, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse und Abhilfebefugnisse verfügt. Von den in der JI-RL aufgeführten Maßnahmen übernimmt der sächsische Gesetzgeber jedoch nur einige.[21] § 40 Abs. 2 Satz 5 SächsDSUG regelt das Recht des Landesdatenschutzbeauftragten, bei erheblichen Verstößen gegen geltendes Recht „geeignete Maßnahmen“ gegen den Verantwortlichen „anzuordnen“. Unklar bleibt dabei, ab welcher Schwelle ein solcher „erheblicher Verstoß“ vorliegen könnte. Hier wird es im Einzelfall auf die Stellung und Ausstattung der Datenschutzaufsicht ankommen, wie weit sie diese Befugnis nutzt. Eine an die JI-RL angepasste Umsetzung hätte – nicht nur in Sachsen (vgl. etwa § 16 Abs. 2 BDSG) – zu einer deutlichen Stärkung der Datenschutzaufsicht über die polizeiliche Datenverarbeitung geführt.[22] Dies wäre auch den An-

19 Sächsischer Landtag: LT-Drs. 6/14791 v. 18.9.2018, S. 263

20 vgl. Kramer, P.; Meints, M.: § 71 BDSG, in: Eßer, M.; Kramer, P.; Lewinski, K.: Auernhammer: DSGVO/BDSG Kommentar, 6. Auflage, Köln 2018, S. 2131 ff. (Rn. 9f.)

21 Sächsischer Landtag: LT-Drs. 6/14791 v. 18.9.2018, S. 267

22 Golla, S.; Michel, A.: Baustellen im polizeilichen Datenschutz – Zur Umsetzung der JIRL in den Ländern, in: JuWissBlog v. 19.3.2019, www.juwiss.de/42-2019

forderungen des Bundesverfassungsgerichts an eine Kontrolle durch Datenschutzbehörden gerade in Bereichen, die mangels offener Durchführung regelmäßig einer gerichtlichen Kontrolle nicht zugeführt werden können, nachgekommen.[23]

Fazit

Im März 2019 konstatierten die Rechtswissenschafter*innen Golla und Michel, der polizeiliche Datenschutz dürfe im Schatten der Anpassung an europarechtliche Umsetzungsforderungen und Polizeirechtsreformen nicht vernachlässigt werden und gaben der Hoffnung Ausdruck, dass in den seinerzeit noch laufenden Gesetzgebungsverfahren sowie in Ergänzung der abgeschlossenen Verfahren Nachbesserungen erfolgten.[24] Diese Hoffnung ist enttäuscht worden. Bei der Umsetzung der JI-RL in den Ländern hat es keinen Schub in Richtung eines verbesserten Datenschutzes bei der polizeilichen Datenverarbeitung gegeben. Die Umsetzung erfolgte weitgehend schematisch und häufig durch bloßes Abschreiben des Wortlauts der Richtlinie, ohne dabei konkrete Umsetzungsschritte und Maßnahmen in die Gesetze aufzunehmen. Dabei wären insbesondere klare gesetzliche Anforderungen an technische und organisatorische Maßnahmen (ggf. im Rahmen einer Verordnungsermächtigung) wichtig, weil effektiver Datenschutz gerade im Bereich der polizeilichen Datenverarbeitung nicht allein mit gesetzlichen Regelungen durchgesetzt werden kann. Mit Blick auf die Datenschutz-Folgenabschätzung (vgl. § 67 BDSG) bedarf es einer deutlich niedrigeren Schwelle für deren verpflichtende Durchführung.[25] Wird hier eine „erhebliche Gefahr für die Rechtsgüter betroffener Personen“ gefordert, führt dies faktisch zu einem (weitestgehenden) Verzicht auf eine solche Folgenabschätzung, zumindest dann, wenn dieser Begriff im polizeirechtlichen Sinne ausgelegt wird.[26]

Die nach der Neubildung der Bundesregierung endlich fällige Umsetzung der JI-Richtlinie auch im Bundespolizeigesetz böte die Chance, ernsthaft neue Maßstäbe zu setzen und „Eckpfosten“ einzurammen. Ein

23 vgl. Bäcker a.a.O. (Fn. 13), S. 76 ff., unter Verweis auf BVerfGE 133, 277 (369); 141, 220 (284)

24 Golla; Michel a.a.O. (Fn. 22)

25 s. Borell, A; Schindler, S.: Polizei und Datenschutz. Vorgaben der neuen JI-RL für technische und organisatorische Maßnahmen zur Gewährleistung datenschutzkonformer polizeilicher Datenverarbeitung, in: Datenschutz und Datensicherheit 2019, H. 12, S. 767-773

26 Schwichtenberg, S.: § 67 BDSG, in: Kühling, J.; Buchner, B. (Hg.): Kommentar Datenschutz-Grundverordnung BDSG Kommentar, 3. Aufl., München 2020, S. 1809ff. (Rn. 2)

Gewinn für den Schutz personenbezogener Daten bei immer weiter ausgreifenden polizeilichen Überwachungsbefugnissen läge dabei sicherlich nicht (allein) in Datenschutz-Folgenabschätzungen oder einer datenschutzfreundlichen Technikgestaltung, sondern im Verzicht etwa auf automatisierte Gesichts- und Verhaltenserkennung, Vorratsdatenspeicherung, die automatisierte Auswertung von Metadaten oder OSINT-Recherchen. Andererseits sind geeignete Regelungen zur Meldung von datenschutzrechtlichen Verstößen gemäß Art. 48 JI-RL erforderlich.

Möglich ist nun aber auch die Kontrolle durch den Europäischen Gerichtshof am Maßstab der EU-Grundrechtecharta, der – wie die Urteile zur Vorratsdatenspeicherung deutlich gemacht haben – unter Umständen besseren Schutz als die deutschen Gerichte einschließlich des Bundesverfassungsgerichts eröffnet. Dies wird es zukünftig strategisch zu testen gelten.