Matthias Pocs

Gestaltung von Fahndungsdateien

Verfassungsverträglichkeit biometrischer Systeme

Um Verdächtige zu finden, setzt die Polizei Kameras ein, die Kfz-Kennzeichen automatisiert erfassen und mit Fahndungsdateien abgleichen. Nach diesem Vorbild werden künftig auch biometrische Systeme eingesetzt. Aufgrund der automatisierten Erfassung und des Inhalts der Referenzdatenbanken können jedoch auch Personen ins Visier der Polizei geraten, die zwar mit Verdächtigen zu tun haben, aber selbst nicht verdächtig sind: Zeugen, Hinweisgeber, Auskunftspersonen, Kontaktpersonen, Opfer usw. Der Beitrag[1] untersucht, wie diese Personen geschützt werden können.

1 Einleitung

An mehreren Stellen des Bahnhofs hängen Kameras, die optisch die Gesichter der Vorbeigehenden erfassen. An den Kameras geht eine Vielzahl von Personen vorbei. Wenn eine Person als Gesuchter erkannt wird, meldet dies das System. Die Meldung wird erzeugt, indem die Gesichtsdaten automatisiert mit polizeilichen Fahndungsdateien abgeglichen werden.

Solch eine Technik hat das Bundeskriminalamt bereits getestet.[2] Bis ihr Einsatz jedoch Wirklichkeit wird, muss die Erfassung und Erkennung biometrischer Charakteristika verbessert werden. Die 2D-Gesichtserkennung hängt stark von äußeren Rahmenbedingungen ab.[3] Die 3D-Gesichtserkennung verspricht, das zu beseitigen.[4]

Außerdem wird erforscht, wie ein Scanner, der Spuren von Fingerabdrücken an Objekten erfasst, zu polizeilichen Zwecken eingesetzt werden kann (Fn 1). Ein fiktives Szenario im Rahmen dieser Forschung ist bereits entwickelt worden.[5] Am Flughafen würden eine Vielzahl von Koffern gescannt und die Fingerspuren an ihnen geortet und erfasst. Sollte ein Fluggast z. B. das Flugzeug zum Absturz bringen, würde auf die Fingerdaten zugegriffen. Die Daten würden dann auch mit Dateien über bekannte Straftäter abgeglichen. Durch den Abgleich könnten der Fluggast und Hintermänner bestimmt werden. Anders als bei der Gesichtserkennung würde erst anlassbezogen auf die Fingerdaten zugegriffen. Da jedoch ein sofortiger Abgleich nach der Erfassung längerfristig möglich zu sein scheint, kann auch vom Einsatz biometrischer Systeme unter Nutzung von Fingerspuren ausgegangen werden.

Eine derartige vorsorgliche Datenerfassung zu polizeilichen Zwecken stellt das Recht vor neue Herausforderungen.[6] Das liegt daran, dass die biometrischen Charakteristika anlasslos und mit großer Streubreite erfasst werden. Dieser Beitrag befasst sich mit der polizeilichen Fahndung mittels biometrischer Systeme und ihrer Auswirkung auf die Personengruppe, die nicht nur von der automatisierten Erfassung, sondern auch von Referenzendatenbanken (und somit von Treffermeldungen) betroffen ist. Es wird untersucht, wie das Grundrecht auf informationelle Selbstbestimmung diese Personengruppen schützt und welche Anforderungen es an die Technikgestaltung stellt.

Matthias Pocs

ist wiss. MA bei provet, war Stagiaire beim Europäischen DSB (P. Hustinx) und studierte als LL.M. IT-Recht in Hannover (Profs. W. Kilian/N. Forgó) und Oslo (Prof. J. Bing/Dr. L. Bygrave); http://provet.uni-kassel.de/pocs
E-Mail: matthias.pocs@uni-kassel.de

2 Grundlagen

Unverdächtige, die sowohl von der Speicherung in Referenzdatenbanken als auch automatisierten Erfassung biometrischer Charakteristika betroffen sind, werden spezifischen Risiken ausgesetzt.

2.1 Fahndungsdateien

Eine Besonderheit biometrischer Polizeisysteme ist, dass eine Fahndungsdatei oder sonstige Referenzdatenbank eingesetzt wird, in der die biometrischen Referenzen zentral gespeichert sind. Diese Zentralisierung ist notwendig, um eine erfasste biometrische Probe mit allen bereits gespeicherten biometrischen Referenzen (Eins-zu-N) zu vergleichen. Beispiele für

1 Die Arbeit, auf der die Ergebnisse in diesem Beitrag beruhen, wurden vom BMBF finanziell gefördert: Projektnr. 13N108 20 – Digitale Fingerspuren (Digi-Dak), http://cms.uni-kassel.de/unicms/index.p hp?id=32301; http://omen.cs.uni-mag deburg.de/digi-dak/

2 Bericht des BKA, http://www.bka.de/kriminal wissenschaften/fotofahndung/pdf/ fotofahndung_ final_report.pdf

3 22. TB des BfDI, S. 84; Heise-News v. 11.07.2007, http://www.heise.de/newsti cker/meldung/BKA-2D-Foto-Fahndung -ist-nicht-einsatzfaehig-150068.html

4 Busch/Nouak, DuD 2008, 126.

5 Hildebrandt/Ulrich/Pocs/Dittmann, BioID 2011 (i. E.).

6 Hornung/Desoi/Pocs, in: Brömme/Busch, BIOSIG 2010, Bonn 2010, S. 83; Hildebrandt, s. o.; zu bisherigen Herausforderungen, Heibey/Quiring-Kock, DuD 2010, 332 m. w. N.

biometrische Referenzdatenbanken sind nationale automatisierte Fingerabdruckidentifikationssysteme (AFIS),[7] die Polizeibehörden aus den Unterzeichnerstaaten des Prümer Vertrags nutzen können,[8] und auf EU-Ebene künftig das Schengen-Informationssystem (SIS) II.[9]

In Bezug auf allgemeine Polizeidatenbanken wurde festgestellt, dass aufgrund der in den letzten Jahren verstärkt eingeführten polizeilichen Ermittlungsbefugnisse, die nicht an eine konkrete Gefahr oder einen Straftatverdacht anknüpfen, der betroffene Personenkreis erweitert wird.[10] Für den Abgleich mit solchen Datenbanken ist bedeutsam, dass jenseits der herkömmlichen Polizeiarbeit zunehmend nicht nur Informationen über Verdächtige erhoben, sondern auch über Personen aus einem ganzen Kriminalitätsbereich, dem Umfeld, der „Szene" und dem gesellschaftlichen Hintergrund, d. h. Anzeigenerstatter, Zeugen und Hinweisgeber oder Personen, die im Kontakt mit verdächtigen Personen oder Organisationen stehen oder bei denen dies angenommen wird.[11]

Eine weitere Besonderheit gegenüber anderen biometrischen Systemen ist, dass der Vergleich ergeben soll, ob eine Person zu den Gesuchten gehört oder nicht. Es wird also eine biometrische Eins-zu-N-Suche auf eine offene Datenmenge („Open Set"-Suche) vorgenommen. Dazu werden biometrische Proben und Referenzen verglichen, um eine Vergleichsentscheidung (Nichtübereinstimmung / Übereinstimmung) oder Kandidatenliste zurückzugeben.[12] Im Folgenden wird die Rückgabe der Vergleichsentscheidung oder Kandidatenliste als „Treffermeldung" bezeichnet.

2.2 Automatische Erfassung

Außerdem stellt die Automatisierung der Erfassungen eine Besonderheit dar. Diese Automatisierung ermöglicht eine Vervielfachung der Erfassungen biometrischer Proben und Vergleiche mit biometrischen Referenzen. Da die anderen Datenverarbeitungsvorgänge, insbesondere der Vergleich, meist bereits automatisiert sind (z. B. bei AFIS), liegt es an der Automatisierung der Erfassungen, dass Referenzdatenbanken für vorsorgliche Datenerfassungen genutzt werden können.

Die einzig bekannte polizeiliche Maßnahme, bei der automatisiert Proben (Kfz-Kennzeichen) erhoben und mit Referenzen (gesuchte Kennzeichen) verglichen werden, ist durch das Bundesverfassungsgericht überprüft worden.[13] Nach Ansicht des BVerfG waren die Gesetzesnormen nicht ausreichend präzise formuliert und erlaubten aufgrund dieser Unbestimmtheit den Abgleich auch mit solchen Referenzdatenbanken (auch wenn dies in der Praxis nicht erfolgte, sondern nur mit „Sachfahndung" und der nationalen SIS-Datei „NSIS-Sachfahndung" aus dem Informationssystem der Polizeien INPOL[14] abgeglichen wurde[15]). Angesichts dieses Fehlens der Zweckbestimmung erklärte das Gericht die Gesetze für verfassungswidrig.[16]

Offen geblieben ist daher die Frage, ob der Einsatz dieser „engeren" Referenzdatenbanken des INPOL im Fall der Kfz-Kennzeichenerfassung zulässig gewesen wäre. Übertragen auf biometrische Systeme ist insbesondere fraglich, welche Personen von Referenzdatenbanken, die für die automatisierte Erfassung biometrischer Charakteristika eingesetzt werden sollen, betroffen sein dürfen.

2.3 Gesteigerte Risikolage

Sollte die Polizei künftig dazu ermächtigt werden, biometrische Charakteristika zum Vergleich mit biometrischen Referenzdatenbanken automatisiert zu erfassen, werden die von den Referenzdatenbanken Betroffenen allgemeinen und spezifischen Risiken ausgesetzt. Zunächst werden die biometrischen Charakteristika automatisiert erfasst. Durch die Automatisierung wird die Zahl der Erfassungen vervielfacht. Diese Vervielfachung steigert das Risiko von Treffermeldungen und möglichen Folgemaßnahmen. Zudem steigert die Vervielfachung die Risiken der Offenbarung sensibler Informationen,[17] Verknüpfung mehrerer Datenbanken zu einem Persönlichkeitsprofil,[18] Gewinnung von Informationen wie Aufenthaltsort, Zeit und Richtung und des unbefugten oder zweckfremden Zugriffs.

Außerdem werden die Betroffenen dem Risiko von falschen Treffermeldungen ausgesetzt. In biometrischen Systemen können die Charakteristika falsch erfasst und zugeordnet werden. Die Falscherfassung und -zuordnung kann auf Lichtverhältnisse, ungeeignete Charakteristika, Überwindungsversuche, Mess-, Bedien- und Verarbeitungsfehler, Entscheidungsregeln des Systems oder Ähnlichkeiten der Charakteristika zweier Personen zurückzuführen sein. Von den Referenzdatenbanken Betroffene könnten somit den erfassten biometrischen Proben und zusätzlichen Informationen fälschlich zugeordnet werden.

Überdies können die Betroffenen diskriminiert werden, weil sie nicht so behandelt werden wie Unbeteiligte, sondern wie potenziell Schwerkriminelle Treffermeldungen und möglichen Folgemaßnahmen ausgesetzt werden können. Diese Diskriminierung kann insbesondere dann nachteilig sein, wenn der Zweck des Systemeinsatzes nachträglich geändert wird. Beispielsweise hat sich herausstellt, dass bei der automatisierten Kfz-Kennzeichenerfassung im Nachhinein andere Zwecke verfolgt wurden (2007: 67 % der Treffermeldungen über Verstöße gegen das Pflichtversicherungsgesetz) als ursprünglich geplant (Bekämpfung grenzüberschreitender Kriminalität, Verhinderung von Anschlusstaten wie Einbrüchen und Unterstützung der Sachfahndung).[19]

Sollten in Zukunft biometrische Systeme zu polizeilichen Zwecken eingesetzt werden, ist zu befürchten, dass Referenzdatenbanken genutzt werden, ohne dass beim Abgleich zwischen den Betroffenen differenziert werden kann. Die technische Unfähigkeit würde also Personen benachteiligen,

- denen eine Gefahr oder Straftat nicht zurechenbar ist,

7 http://www.bka.de/pressemitteilungen/hintergrund/hintergrund2.html

8 EU-Ratsbeschlüsse 2008/615/JI und 2008/616/JI, ABl. EU L 210, 1 bzw. 12; 2010/482/EU, ABl. EU L 238, 1.

9 EU-Ratsbeschluss 2007/533/JI, ABl. EU L 205, 63; EG-Verordnung 1987/2006, Abl. EU L 381, 4.

10 Petri in: Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., H. 67 und 68.

11 BVerfGE 120, 378 (411) – Automatisierte Kennzeichenerfassung, http://www.ser vat.unibe.ch/dfr/; s. auch z. B. § 20b Abs. 2 BKA-G und für ED-Daten § 8 Abs. 4 BKA-G..

12 Zur Terminologie, ISO SC37 Harmonized Biometric Vocabulary (SD 2 V. 12) in SC37 WG 1.

13 BVerfGE 120, 378.

14 §§ 2 Abs. 3 und 11 Abs. 1 BKA-G.

15 Hessische Staatskanzlei auf Fragen des BVerfG, 23. Oktober 2007, http://www. daten-speicherung.de/data/Hessen_ Antworten_2007-10-23.pdf, S. 10.

16 BVerfGE 120, 378.

17 Sensible Informationen könnten offenbart werden, Artikel-29-DS-Gruppe: WP80, Punkt 3.7.

18 Datenbanken könnten verknüpft werden, Artikel-29-DS-Gruppe, s. o., Punkt 3.2.

19 Bodenbenner, NVwZ 2010, 679.

- gegen die sich ein Verdacht nicht ausreichend verdichtet hat,
- die einer Gefahr für oder Straftat gegen hochrangige Rechtsgüter nicht verdächtig sind und
- die eine Tat von geringem Unrechtsgehalt begangen haben.

Diese „anderen Personen" können nämlich genau wie potenziell Schwerkriminelle von Treffermeldungen und möglichen Folgemaßnahmen betroffen werden. Da Treffermeldungen vom Umfang der Referenzdatenbank abhängen, ist zu untersuchen, welche Regelungen zur Gestaltung von Referenzdatenbanken bei einer automatisierten Erfassung biometrischer Charakteristika das Grundrecht auf informationelle Selbstbestimmung vorgibt.

3 Grundrechtsschutz für die „anderen Personen"

Durch den Einsatz des biometrischen Polizeisystems könnte in Grundrechte von Betroffenen eingegriffen werden. Infrage kommt insbesondere ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[20] Zunächst sind die Daten personenbezogen, weil die biometrischen Proben den Referenzen zugeordnet werden können und die biometrischen Referenzen in einer Referenzdatenbank gespeichert sind, die das Auffinden von Personen ermöglichen soll. Außerdem fallen die Datenverarbeitungsvorgänge in den Anwendungsbereich des Grundrechts auf informationelle Selbstbestimmung, weil zum einen biometrische Proben erhoben, übermittelt, zusammengeführt und abgeglichen[21] und zum anderen biometrische Referenzen für den Vergleich genutzt werden.[22]

Ein Grundrechtseingriff kann durch Zwecke gerechtfertigt werden, die dem Allgemeininteresse dienen. Polizeiliche Zwecke können grundsätzlich einen hohen Verfassungsrang genießen.[23] Außerdem ist das biometrische System zur Gefahrenabwehr und Strafverfolgung geeignet, weil durch ihren Einsatz zweckent-

20 Jüngst BVerfG, 2 BvR 1372/07, Abs. 18 – Mikado; ständige Rechtspr. seit BVerfGE 65, 1 – Volkszählungsurteil.

21 Als relevant eingestuft in BVerfGE 115, 320 (360) – Rasterfahndung II.

22 Als relevant eingestuft in BVerfGE 115, 320 (344); BVerfGE 100, 313 (366) – TKÜ I.

23 So in BVerfGE 120, 378 (427).

sprechende Maßnahmen möglich oder einfacher werden, und erforderlich, weil die Zahl der Erfassungen eine neuartige Reichweite polizeilicher Beobachtung ermöglicht.[24] Allerdings bestehen auch bei geeigneten und erforderlichen Maßnahmen zu legitimen Zwecken bestimmte Grenzen: Zum einen muss das Gesetz so präzise formuliert sein, dass vorauszusehen ist, zu welchen Zwecken das biometrische System eingesetzt werden soll.[25] Außerdem müssen unangemessene Grundrechtseingriffe vermieden werden.

3.1 Eingriff durch Treffermeldung

Bei der Beurteilung der Angemessenheit sind die Schwere der Beeinträchtigung für die Betroffenen und das Gewicht der verfolgten Interessen miteinander abzuwägen. Dabei helfen die Prinzipien des Datenschutzrechts. Zunächst sind von der Erfassung biometrischer Proben Personen betroffen, die keinen Anlass für biometrische Vergleiche geschaffen haben (Zweckbestimmung). Zudem erhöht die Heimlichkeit des Systemeinsatzes das Gewicht des Grundrechtseingriffs (Transparenz). Dadurch wird ein Gefühl des Überwachtwerdens verursacht, aufgrund dessen der Betroffene seine Grundrechte eventuell nicht frei ausübt.[26] Überdies können sensible Informationen offenbart werden (Sensibilität). Diese Eingriffsvertiefung bezieht sich sowohl auf die Erfassung und Übermittlung der biometrischen Probe als auch ihre Nutzung für den biometrischen Vergleich. Durch rechtlich und technisch gesicherte Löschung kann das Eingriffsgewicht verringert werden (Technikgestaltung, s. u.). Dieses Eingriffsgewicht gilt bereits für die Personen, die lediglich von der Erfassung und Nutzung biometrischer Proben betroffen sind (in der Datenbank sind keine auf sie bezogene Referenzen).

Das Gewicht für den Eingriff bei den „anderen Personen", welche zusätzlich von der Nutzung biometrischer Referenzen betroffen sind, wird sogar noch erhöht. Zunächst sind sie von Treffermeldungen und möglichen Folgemaßnahmen betroffen, für die sie keinen Anlass geschaffen haben (Zweckbindung). Des Weiteren können ihnen Treffermeldungen falsch zugeordnet werden (Datenrichtigkeit[27]). Außerdem können sie von Treffermeldungen betroffen sein wie potenziell Schwerkriminelle (Treu und Glauben[28] und Gleichbehandlung[29]). Die spezifische Eingriffsvertiefung bezieht sich insbesondere auf die Nutzung der biometrischen Referenzen für den biometrischen Vergleich.

Hinzu kommt eine gesellschaftliche Dimension: Das Grundrecht auf informationelle Selbstbestimmung dient nicht nur dem Schutz Einzelner, sondern auch dem Gemeinwohl, weil „Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist".[30] Ein Eingriff kann also auch aus gesellschaftlichen Gründen tiefer sein, als dies bei einer Betrachtung des individuellen Eingriffs der Fall wäre. Daher stellt das Bundesverfassungsgericht bei vorsorglicher Datenerfassung zu polizeilichen Zwecken fest, dass eine Vielzahl von Betroffenen, die keinen Anlass für die Verarbeitung geschaffen haben, den Eingriff vertieft (Streubreite[31]). Diese Eingriffsvertiefung bezieht sich auf die Erfassung und Nutzung der Proben. Jedoch kann sie sich abhängig von der Zahl der „anderen Personen" auch auf die Nutzung der biometrischen Referenzen beziehen. Insgesamt lässt sich festhalten, dass die Eingriffstiefe aus individuellen und gesellschaftlichen Gründen als hoch einzustufen wäre.

3.2 Zweckbestimmung

Aufgrund des Bestimmtheitsgebots und der oben bewerteten Eingriffstiefe muss der Zweck des Einsatzes eines biometrischen Polizeisystems so präzise festgelegt werden, dass der Grundrechtseingriff bei den „anderen Personen" ausgeschlossen ist. Zunächst müssten Treffermeldungen über Personen ausgeschlossen werden, denen eine Gefahr oder Straftat nicht zurechenbar ist. Außerdem müssten auch Personen, denen eine Gefahr oder Straftat nicht mehr zurechenbar ist, verschont bleiben, d. h., wenn gegen sie erfolglos ermittelt worden ist oder ein Restverdacht nach Beendigung des Strafverfahrens nicht besteht. Des Weiteren könnten nur konkrete Gefahren oder Anfangsverdachte einer Straftat eine Treffermeldung rechtfertigen. Anfangsverdachte sind nur dann begründet, wenn die Tatsachen nicht nur unerheblich sind, über bloße Vermutungen hinausreichen, sich auf die „äußere oder innere Geschehenswelt" beziehen und auf kriminalistischen Erfahrungen basieren.[32]

Überdies muss der Zweck bestimmt werden, indem ausdrücklich festgelegt wird, welche Rechtsgüter mit dem Einsatz des biometrischen Systems geschützt werden sollen. Abstufungen des Rechtsgutsrangs wurden bisher anhand der Erheblichkeit[33] oder der besonderen Schwere[34] vorgenommen. Bei besonderer Schwere sind die Straftaten anhand des Strafrahmens konkret zu benennen.[35] Für die Gefahrenabwehr sind die Rechtsgüter konkret benannt, wenn Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person abgewehrt werden sollen.[36] Außerdem muss der Einsatz des biometrischen Systems so begrenzt werden, dass es auf den Unrechtsgehalt der Tat im Einzelfall ankommt. Ein überdurchschnittlicher Unrechtsgehalt ist zwar bei bestimmten Straftaten grundsätzlich anzunehmen.[37] Im Einzelfall könnten jedoch auch weniger schwere Straftaten den Einsatz rechtfertigen.[38]

Sollten in Zukunft biometrische Systeme zu polizeilichen Zwecken eingesetzt werden, würde eine Technikgestaltung gefordert, die eine Differenzierung zwischen den Betroffenen erlaubt. Die Verarbeitung der biometrischen Proben und Referenzen sowie die Treffermeldungen würden nämlich besonders intensiv in das Grundrecht auf informationelle Selbstbestimmung der „anderen Personen" eingreifen. Die Begrenzung auf Zurechenbarkeit, ausreichende Tatsachenbasen, hohe Rechtsgüter und Unrechtsgehalte bieten Rechtsschutz

24 So in BVerfGE 120, 378 (428).
25 z. B. BVerfGE 120, 378 (424).
26 BVerfGE 120, 378 (402); BVerfG, 2 BvR 1345/03, Abs. 65 – IMSI-Catcher; BVerfGE 115, 320 (342); 115, 166 (188) – E-Mail; 113, 29 (46) – Anwaltsdaten; 65, 1 (42).
27 Datenrichtigkeit (i. e. S.), -aktualität, und -vollständigkeit nach Art. 6 Buchst. d DS-Rili 95/46/EG und Art. 5 Buchst. d DS-Übereinkommen SEV Nr. 108; auch Abs. 8 OECD-DS-Leitlinien 1980.
28 Art. 6 Buchst. a DS-Rili und Art. 5 Buchst. a DS-Übereinkommen; auch Abs. 7 OECD-DS-Leitlinien.
29 Art. 6 Abs. 2 The Madrid Resolution, http://www.privacyconference2009.org/media/Publicaciones/common/estanda res_resolucion_madrid_en.pdf
30 BVerfGE 65, 1 (43); 100, 313 (381).
31 BVerfGE 120, 378 (402); 115, 320 (354 f.); 107, 299 (328) – Zielwahlsuche.
32 Meyer-Goßner, 50. Aufl., § 100a StPO, Rn. 9.
33 z. B. BVerfGE 107, 299.
34 z. B. BVerfGE 109, 279 – G. Lauschangriff.
35 BVerfGE 109, 279 (348f.).
36 BVerfGE 115, 320 (365f.).
37 BVerfGE 109, 279 (346ff.).
38 BVerfGE 107, 299 (Abs. 81f.).

für die Personen, die nicht als potenziell Schwerkriminelle infrage kommen. Diese Zweckbestimmung kann nur durchgesetzt werden, wenn die Referenzdatenbank so gestaltet wird, dass beim Abgleich zwischen den Betroffenen differenziert werden kann.

4 Gestaltung der Referenzdatenbank

Die Zweckbestimmung zum Schutz für die „anderen Personen" vor Treffermeldungen wäre unwirksam, wenn die biometrische Referenzdatenbank nicht zweckentsprechend gestaltet würde. Erforderlich können daher gesetzliche Regelungen sein, die eine Gewährleistung der Zweckbestimmung durch Technikgestaltung in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben.[39] Das Prinzip der Technikgestaltung („Privacy by Design"[40]) zielt darauf ab, die Einhaltung der Datenschutzprinzipien durch technisch-organisatorische Maßnahmen des Gestalters zu gewährleisten. An die konkrete Technikgestaltung werden unmittelbar Rechtsfolgen geknüpft; z. B. verhindert bei der automatisierten Kfz-Kennzeichenerfassung die Technikgestaltung den Eingriff in das Grundrecht auf informationelle Selbstbestimmung bei denen, die durch das sofortige und spurenlose Löschen der erfassten Daten geschützt werden.[41]

Einige Ausprägungen des Prinzips der Technikgestaltung sind bereits entwickelt worden.[42] Der Systemdatenschutz ist so umfassend konzipiert wie „Privacy by Design" und regelt insbesondere, dass bei einer gemeinsam genutzten Datenbank die Zweckbindung durchgesetzt wird, indem die Verfügung über die Datenbank einer vertrauenswürdigen Behörde zugewiesen wird und diese Behörde zweckentsprechende Benutzerrechte an die zugreifenden Behörden vergibt.[43] Das Konzept der Datenvermeidung und Datensparsamkeit regelt insbesondere, dass Systeme so gestaltet werden, dass Daten möglichst (abhängig vom Zweck und der Angemessenheit) ohne Personenbezug erhoben werden, ihr Umfang während der Verwendung verringert wird und ihre Speicherdauer verkürzt wird.[44] Das Konzept kombiniert also die Prinzipien der Datenminimalität[45] und Technikgestaltung. Beispielsweise ist das Konzept wichtig, um auszuschließen, dass Daten über Personen gespeichert werden, denen eine konkrete Gefahr oder Straftat nicht mehr zurechenbar ist.[46]

4.1 Betroffenendifferenzierung

Die Ausprägungen des Prinzips der Technikgestaltung reichen allerdings nicht aus. Sie reichen nur in Anwendungen, für die der Einzelne Anlass gegeben hat. Das System kann dann nämlich so gestaltet werden kann, dass der Umfang anhand dieses Anlasses (der Zweckbestimmung) reduziert wird. Bei vorsorglicher Datenerfassung zu polizeilichen Zwecken haben die Betroffenen keinen Anlass für die Treffermeldung gegeben. Um zwischen Verdächtigen und „anderen Personen" unterscheiden zu können, muss die Referenzdatenbank so gestaltet sein, dass zweckentsprechend zwischen den Betroffenen differenziert werden kann.[47]

Die zweckwidrigen Vergleiche resultieren somit aus der Gestaltung der Referenzdatenbanken, welche eine Datenbasis, die ausreicht, um Treffermeldungen auf sie zu stützen, nicht zulässt. Es fehlen die notwendigen Datenfelder. Somit wird verhindert, dass die zur Zweckbindung erforderlichen Kategorien von Informationen (z. B. Eigenschaft des Betroffenen als Zeuge oder Begleitperson) erfasst werden können. Ähnliches gilt für die Unterscheidung von Vermutungen und verdachtsbegründenden Tatsachen. Die Informationen über Betroffene sind unvollständig und die Treffermeldungen falsch, da der Betroffene nach der Zweckbestimmung nicht von der Treffermeldung betroffen sein dürfte. Das verletzt das Prinzip der Datenrichtigkeit.

Demgegenüber könnten zweckwidrige Treffermeldungen verhindert werden, indem die Systeme so gestaltet werden, dass die Kategorien von Informationen, die zur zweckentsprechenden Differenzierung zwischen Betroffenen erforderlich sind, erfasst werden können. Solch eine Betroffenendifferenzierung würde folglich die Prinzipien der Datenrichtigkeit und Technikgestaltung kombinieren.

Zweckwidrige Treffermeldungen sind nur dann auszuschließen, wenn für die Datensätze der Referenzdatenbank besondere Felder definiert sind. Im System könnte dann geregelt werden, welche Werte die Felder haben sollen, um zu entscheiden, ob der konkrete Datensatz für den Vergleich eingesetzt werden soll. Durch die Felder und das Regelwerk wird somit die Erfüllung der zweckentsprechenden Betroffenendifferenzierung ermöglicht.

Es ist fraglich, ob die in der Praxis eingesetzten Systeme die Anforderungen einer zweckentsprechenden Betroffenendifferenzierung erfüllen können. Da die automatisierte Kfz-Kennzeichenerfassung der erste Systemeinsatz ist, der dem Einsatz eines biometrischen Polizeisystems ähnelt, wird im Folgenden die Gestaltung der tatsächlich eingesetzten Referenzdatenbanken, die INPOL-Dateien „Sachfahndung" und „NSIS-Sachfahndung", untersucht.

Das sog. Feld „N24" in „Sachfahndung" erlaubt, den „Anlass" einer Ausschreibung festzulegen.[48] Die „Anlässe" sind: Abhandengekommen, Haftpflichtversicherung, Amts-/Vollzugshilfe, sonstige Gefahrenabwehr, Benutzung, polizeiliche Beobachtung, sonstiger Anlass und Gefährder. Diese Anlässe werden durch Hinweisfelder ergänzt. Einige „Anlässe" dienen also grundsätzlich nicht besonders hohen Rechtsgütern. Andere sind Auffangwerte („sonstige Gefahrenabwehr"). Zusätzlich wird der „Zweck" der Ausschreibung, z. B. Beweis-, Eigentumssicherung oder Entstempelung, in Feld „N25" festgelegt.

Der Anlass „polizeiliche Beobachtung" wird weiter in einzelne Anlässe aufgeschlüsselt: zum einen in den Auffang-

39 In Anlehnung an BVerfG, 1 BvR 256/08, Abs. 225 – Vorratsdatenspeicherung.

40 Zur Aufnahme des Prinzips der Technikgestaltung als Regelung der künftigen EU-Datenschutzrichtlinie, Artikel-29-DS-Gruppe: WP168, Abs. 46.

41 BVerfGE 120, 378 (411); umstritten, Guckelberger, NVwZ 2009, 352, Fn 70 m. W. N.

42 Information and Privacy Commissioner of Ontario Canada: Privacy By Design – Take The Challenge 2009, http://www. privacybydesign.ca/content/uploads/ 2010/03/PrivacybyDesignBook.pdf; Bygrave: Data Protection Law 2002, Fn 1234 m. W. N.

43 Dix in: Roßnagel, Handbuch des Datenschutzrechts 2003; Steinmüller, Informationstechnologie und Gesellschaft 1993, S. 671; Podlech in: Brückner/Dalichau, Festgabe für Hans Grüner 1982, 452 ff.

44 Roßnagel in: Eifert/Hoffmann-Riem, Innovationsrecht und Informations- und Kommunikationstechnologien (i. E.); das Prinzip normiert z. B. § 3a BDSG.

45 Nach Art. 6 Buchst. c und e DS-Rili und Art. 5 c und e DS-Übereinkommen.

46 S. auch 28. TB 2007 des LfD BW, Punkt 3, http://www.baden-wuerttemberg.daten schutz.de/lfd/tb/2007/tb-2.htm

47 Das wird womöglich in der künftigen DS-Rili geregelt, COM(2010) 609 endg., Punkt 2.3 Abs. 3.

48 Hessische Staatskanzlei, Fn 15.

wert „sonstige Gefahrenabwehr“, zum anderen in einzelne Delikte. Dieser Anknüpfungspunkt beschränkt die polizeiliche Beobachtung jedoch nicht auf Verdächtige. Wie beispielsweise durch § 163e StPO zugelassen können auch Kontaktpersonen von der polizeilichen Beobachtung betroffen sein. Bei der Personenfahndung[49] würde die Aufenthaltsermittlung nach Art. 98 SDÜ[50] und in Deutschland z. B. nach § 131a StPO, welche auch Zeugen betreffen kann, hinzukommen.

Es ist deshalb festzustellen, dass die Gestaltung der Referenzdatenbanken, die für die automatisierte Kfz-Kennzeichenerfassung eingesetzt werden, für den Einsatz in biometrischen Systemen nicht zulässig ist. Sie würde keine zweckentsprechende Betroffenendifferenzierung ermöglichen. Auch durch Kombinationen der Felder N24 und N25 kann eine Treffermeldung höchstens auf Delikte aus dem mittleren Kriminalitätsbereich oder auf Eigenschaften wie „internationaler Täter“ und „kriminelle Vereinigung“ beschränkt werden. Auffangwerte wie „sonstige Gefahrenabwehr“ sagen nichts über den Rang des zu schützenden Rechtsguts aus. Eventuell könnten in den Hinweisfeldern Daten darüber eingegeben werden, wie hoch das Rechtsgut und der Unrechtsgehalt einzustufen sind und ob es sich um einen Verdächtigen oder Nichtverdächtigen handelt. Ob sich die Hinweisfelder jedoch eignen würden, um zu entscheiden, ob der konkrete Datensatz für den biometrischen Vergleich eingesetzt werden soll, ist zweifelhaft, insbesondere weil sie nicht immer zwingend und ihre Werte nicht standardisiert sind. Daher wäre für den Einsatz eines biometrischen Polizeisystems die Definition von Feldern erforderlich, durch die das Vorliegen einer Gefahr für oder Straftat gegen besonders hohe Rechtsgüter, einer Straftat mit äußerst großem Schadensausmaß und die Eigenschaft als Verdächtiger oder Nichtverdächtiger zu bestimmen ist.

49 Für SIS, EU-Rat: C.SIS at 01/01/2010, 6162/10 SIS-TECH 18 SIRIS 22 COMIX 103, 5. Februar 2010.

50 Schengen-Durchführungsübereinkommen, BGBl. 1993 II S. 1010.

4.2 Rechenschaft durch Technik

Zweckwidrige Treffermeldungen sind außerdem nur dann auszuschließen, wenn die tatsächliche Einhaltung der zweckentsprechenden Betroffenendifferenzierung überprüft werden kann. Wenn der Betroffene (oder ein Richter) nicht von der Verwaltungsentscheidung vor der Ausschreibung erfährt, fehlt der Schutz durch gerichtliche Überprüfung dieser Entscheidung. Aus diesem Grund werden besondere Transparenz- und Rechtsschutzanforderungen aufgestellt.[51] Diese Anforderungen können nur erfüllt werden, wenn nachweisbar Rechenschaft über die Datenverwendung gegenüber der Kontrollinstanz des biometrischen Systems abgelegt werden kann (Datenschutzmanagement).[52]

Um Rechenschaft darüber ablegen zu können, ob die biometrische Referenzdatenbank auch tatsächlich so verwendet wird, dass zweckentsprechend zwischen den Betroffenen differenziert wird, muss die Referenzdatenbank so gestaltet sein, dass sie nachweisen kann, welche Datensätze für den biometrischen Vergleich eingesetzt werden. Ohne solch eine Gestaltung ist es der Polizei nicht möglich, ihre Rechenschaftspflicht bezüglich der Treffermeldungen zu erfüllen.

Solch eine „Rechenschaft durch Technik“ („Accountability by Design“) könnte durch Zählung der Personen, die von Treffermeldungen betroffen werden können, gewährleistet werden:

Es wird ein Auswertefeld definiert, das die für den biometrischen Vergleich eingesetzten Referenzdatensätze zählt. Die Zahl der Datensätze könnte Grundlage für eine Benachrichtigung der Kontrollinstanz sein (z. B. über Schwellwerte). Eine äußerst große Zahl von Referenzdatensätzen könnte nämlich Zweifel daran begründen, dass die Verarbeitung von Daten zweckentsprechend begrenzt wird. Die Benachrichtigung ist zwar keine „Datenverletzungsb enachrichtigung“,[53] jedoch könnte sie die Entscheidung der Kontrollinstanz über die Prioritäten geplanter Untersuchungen beeinflussen. Zudem ist die Zahl der Datensätze notwendig für die Neubewertung von Gesetzen und Maßnahmen, insbesondere weil nicht „ins Blaue hinein“ ermittelt werden darf[54] und der Gesetzgeber notfalls durch ergänzende Rechtssetzung korrigierend eingreifen muss.[55] Solch eine „Rechenschaft durch Technik“ wäre also Datenschutz fördernd, weil sie die Aufmerksamkeit auf biometrische Referenzdatenbanken lenken würde, bei denen eine Untersuchung der Einhaltung der zweckentsprechenden Betroffenendifferenzierung oder eine Gesetzesevaluierung sinnvoll ist.

51 BVerfG, 1 BvR 256/08, Abs. 239 m. w. N.

52 Zur Aufnahme einer Rechenschaftspflicht in die künftige DS-Rili, Artikel-29-DS-Gruppe: Opinion 3/2010 (WP 173), 13. Juli 2010; früh bereits Abs. 12 OECD-DS-Leitlinien 1980.

53 Nach Art. 4 Abs. 3 Satz 2 Rili 2002/58/EG eingefügt durch Rili 2009/136/EG, ABl. EU L 337 v. 18.12.2009, 11.

5 Fazit

Bei automatisierter Erfassung biometrischer Charakteristika würden Referenzdatenbanken besonders intensiv genutzt. Das würde zu einem neuartigen Risiko von Treffermeldungen und möglichen Folgemaßnahmen führen. Treffermeldungen über Personen wie Zeugen, Kontaktpersonen u. a. können nur durch die Technikgestaltung ausgeschlossen werden. Eine Nutzung der Referenzdatenbanken in ihrer gegenwärtigen Gestalt wäre unzulässig. Wenn Strafverfolgung und Gefahrenabwehr durch Automatisierung der Erfassung effektiviert werden sollen, muss auch der Schutz der Grundrechte von Personen effektiviert werden, die zweckwidrig von Treffermeldungen und möglichen Folgemaßnahmen betroffen sind.

Solch eine Effektivierung des Grundrechtsschutzes ist möglich. Eine datenschutzrechtliche Überprüfung kann das Argument für den Einsatz biometrischer Systeme nur stärken. Denn der vernünftige Bürger ist an beidem interessiert: Schutz vor Gefahren und Straftaten und Schutz vor Folgen des Missbrauchs informationeller Macht. Wenn die Gestaltungsmöglichkeit genutzt wird, kann das Fundament für eine Zukunft gelegt werden, die sich die Gesellschaft wünscht.

54 z. B. BVerfGE 120, 378 (429); 115, 320 (360 f.) m. w. N.

55 BVerfGE 112, 304 – GPS.