



Chaos Computer Club

Stellungnahme an den Innen- und Rechtsausschuss
des Schleswig-Holsteinischen Landtags

Entwurf eines Gesetzes zur Fortentwicklung
polizeirechtlicher Maßnahmen für einen wirksamen
Schutz der öffentlichen Sicherheit

Drucksache 20/4284

Dirk Engling, Constanze Kurz, Matthias Marx

9. September 2026

Vorbemerkung	3
1. Automatisierte Datenanalyse	3
Zusammenführung und Analyse personenbezogener Datenbestände	3
Auffälligkeiten und Diskriminierung	4
Technisches System ohne Details	4
2. Verhaltensscanner	5
Grenzfälle der Mustererkennung	5
3. Biometrische Fernidentifikation	6
Keine Anonymität mehr in der Öffentlichkeit	8
Nachträglicher Abgleich	8
Biometrische Massenüberwachung	9
Neue Befugnisse zusammen betrachtet	9
Fazit.....	11

Vorbemerkung

Diese Stellungnahme widmet sich einem Teil der im Gesetzentwurf enthaltenen neuen Regelungen. Der Entwurf enthält Befugnisse zur Gefahrenabwehr, die in ihrer Reichweite und technischen Ausgestaltung an Gesetze anderer Bundesländer anknüpfen, die das Bundesverfassungsgericht bereits 2023 aufgrund von unzureichender qualitativer und quantitativer gesetzlicher Begrenzung für verfassungswidrig erklärt hat. Insbesondere die Vereinbarkeit der geplanten neuen Befugnisse zur automatisierten Datenanalyse, aber auch die Befugnisse zu Verhaltensscannern – also automatisierter Anwendungen zur Mustererkennung von Bewegungs- und Verhaltensmustern – und die biometrische Fernidentifikation sind nur schwer mit dem Grundgesetz zu vereinbaren.

Begründet wird die Notwendigkeit der vorliegenden Gesetzesänderung in der Problembeschreibung des Entwurfs durch einen Anstieg der verzeichneten Messerangriffe als mehrfach erwähntes Beispiel der zu verhindernden Gefahrenlagen. Hier stellen sich mehrere Fragen: Welche konkrete Schutzlücke bei Messerangriffen oder anderen konkreten Gefahrenlagen soll durch welche konkrete technische Befugnis geschlossen werden? Sind die Maßnahmen erforderlich und überhaupt geeignet, Messerangriffe zu verhindern? Wie soll die Wirksamkeit des Gesetzes in Hinsicht auf dieses Ziel evaluiert werden? Der vorliegende Entwurf liefert auf keine dieser Fragen adäquate Antworten.

1. Automatisierte Datenanalyse

Zusammenführung und Analyse personenbezogener Datenbestände

Der Entwurf erlaubt in § 188c ausdrücklich die automatisierte Zusammenführung und Analyse verfügbarer personenbezogener Datenbestände zur Gewinnung neuer Erkenntnisse. Dabei können neben polizeilichen Datenbeständen auch gezielt abgefragte Daten aus externen staatlichen Registern, Asservaten und anderen Beweismitteln sowie öffentlich zugängliche Quellen einbezogen werden. Damit wird aus bislang getrennten Datenbeständen eine neue polizeiliche Wissensinfrastruktur.

Der Entwurf verwendet selbst die Formulierung, dass durch die Zusammenführung neue Strukturen, Muster und Zusammenhänge sichtbar würden. Das beschreibt genau die Folgen der Datenanalyse, die vom Bundesverfassungsgericht als besonders eingriffsintensiv klassifiziert wurde. Bei einer so weitreichenden Datenzusammenführung kommen unweigerlich zahlreiche unbeteiligte Menschen ins Visier.

Die Gefahr der automatisierten Datenanalyse liegt zudem in ihrer Permanenz. Ist sie einmal angestoßen, läuft sie beständig im Hintergrund. Jede Änderung in den zugrunde liegenden Datenbeständen löst eine Neubewertung durch die Software aus. Durch die Zusammenführung der Daten geschieht diese softwareseitige Aufbereitung im Hintergrund auch dann, wenn keine neue Nutzeranfrage zur Analyse gestellt werden. Es handelt sich also um eine ständige Verarbeitung und Auswertung aller eingebundenen Daten.

Eine wirksame Kontrolle der Datenverarbeitung und der Verarbeitungsmethoden sicherzustellen, erweist sich daher als problematisch. Die Zugriffe auf die

Anwendung des Systems können zwar protokolliert werden, nicht erfasst wird dabei allerdings die eigentliche permanente Datenverarbeitung innerhalb des Systems.

Eine gesetzliche Erlaubnis zu solchen automatisierten Datenanalysen kommt wegen der grundrechtlichen Eingriffstiefe und wegen der zahlreichen betroffenen Unbeteiligten nur bei sehr schwerwiegenden Rechtsgutverletzungen überhaupt in Frage. Auch dann müsste die Analyse durch klare und eng gezogene Regeln begrenzt werden.

Auffälligkeiten und Diskriminierung

Ein typisches Analysesystem sucht nach statistischen Auffälligkeiten und Zusammenhängen in den zur Verfügung gestellten Daten. Sind diese Daten bereits verzerrt, beispielsweise durch frühere polizeiliche Maßnahmen, kann das System diese Verzerrung erlernen und verstärken.

Wird eine Gruppe mit bestimmten Merkmalen häufiger kontrolliert und deshalb häufiger in polizeilichen Datenbeständen erfasst, kann ein Analyseverfahren daraus eine statistische Auffälligkeit dieser Gruppe ableiten. Dieses Problem betrifft sowohl KI-gestützte als auch traditionell regelbasierte Software. Diese Auffälligkeit kann wiederum zu weiteren Kontrollen führen, wodurch erneut mehr Daten über dieselbe Gruppe entstehen. So kann ein Kreislauf entstehen, in dem eine anfängliche Verzerrung – auch ohne jegliche Diskriminierungsabsicht – durch automatisierte Analysen verstärkt wird.

Andersrum gilt aber auch: Ein System kann nur Zusammenhänge erkennen, die sich in den verfügbaren Daten abbilden. Wer besonders viele digitale oder polizeiliche Spuren hinterlässt, erscheint deshalb unter Umständen auch besonders „erkenntnisreich“. Wer seine Spuren vermeiden kann, erscheint dagegen nicht als unbekannt, sondern schlicht als weniger sichtbar. Ein Datenanalysesystem findet nicht notwendigerweise diejenigen, die tatsächlich relevant sind. Es findet denjenigen Zusammenhang, der in den verfügbaren Daten am deutlichsten hervortritt.

Je scheinbar deutlicher und treffsicherer ein System Verdächtige hervorbringt, desto leichter kann gerade der daraus resultierende Erfolgseindruck dazu führen, dass die Ergebnisse weniger kritisch hinterfragt werden. Je mehr Vertrauen in die Leistungsfähigkeit des Systems, desto weniger Anlass gibt es, die vorgeschlagenen Zusammenhänge selbst zu hinterfragen. Auch ausgebildete und gutwillige Menschen neigen dazu, einer maschinell erzeugten Information zu viel Gewicht beizumessen, wenn sie deren Entstehung und Fehlerwahrscheinlichkeit nicht beurteilen können.

Technisches System ohne Details

Das Bundesverfassungsgericht warnte ausdrücklich davor, dass die automatisierte Datenanalyse die Ziele der Polizeiarbeit auf Kontaktperson, Zeugen oder Geschädigte bloß aufgrund eines sachlichen Zusammenhangs zu gespeicherten Personen ausweitet. Es stellte daher klar: Die Datenanalyse erzeugt neues Wissen.¹ Je umfangreicher und methodenoffener die Analyse ist, desto strikter müssen die

¹ 1 BvR 1547/19, 1 BvR 2634/20, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html, abgerufen: 9. September 2026.

Schranken werden. Im Gesetzentwurf werden diese Schranken jedoch vielfach auf Verwaltungsvorschriften verschoben.

Konkret welche zuvor unverknüpften Daten zusammen analysiert werden dürfen, wie Gewichtung gestaltet sind, welche Verknüpfungen als relevant angesehen werden oder welche Schwellenwerte für Treffer gelten, wird im Entwurf nicht vorgegeben, sondern wird erst durch Konfigurationen, Training, Updates und bei einem Kauf entsprechender Software durch Anbieterentscheidung bestimmt. Damit hängt der tatsächliche Grundrechtseingriff nicht vom Gesetz ab, sondern von den technischen Details der Verwaltungsvorschriften und von der Umsetzung, die nicht transparent sind und zudem einer ständigen Veränderung unterliegen können.

Dies ist aus Sicht einer effektiven Kontrolle besonders problematisch. Die genaue technisch-organisatorische Ausgestaltung von essentiellen Einzelheiten, darunter Suchkriterien, Zugriffsrechte, Protokollierung, technische Sicherungen und Speicherfristen, soll erst später durch Verwaltungsvorschriften geregelt werden. Doch genau dieser Ausgestaltung bemisst sich die vom Bundesverfassungsgericht normierte Eingriffstiefe des Vorhabens.

Die Vorgaben im Entwurf enthalten keine Details, das technische System darf daher auf nicht näher spezifizierte Weise die heterogenen Polizeidaten in einer beliebigen Art analysieren und bewerten, um etwas herauszufinden, was ebenfalls nicht erkennbar definiert ist. Kein wesentliches Element des Analysesystems ist damit durch den Gesetzentwurf bestimmt.

2. Verhaltensscanner

Der Gesetzentwurf sieht in § 184 Absatz 5 vor, dass der Polizei zusätzlich zur Videoüberwachung automatisierte Anwendungen zur Mustererkennung in den Aufnahmen erlaubt werden sollen. Die neue Befugnis soll vereinfacht gesprochen den Einsatz einer automatisierten Anwendung erlauben, die permanent Aufnahmen der Videokameras dahingehend prüft, ob vorab vorgegebene Verhaltens- oder Bewegungsmuster erkannt werden. Ein Mensch soll die Ergebnisse der Software im Fall der Markierung einer aufgezeichneten Situation sichten, dann die potentielle Gefahr bewerten und gegebenenfalls Maßnahmen gegen abgebildete Personen einleiten.

Die offensichtliche Frage für jeden dieser Verhaltensscanner lautet daher: Wer legt diese Muster fest, auf welcher empirischen Grundlage und mit welcher Fehlerquote? Der Mensch prüft nämlich nicht mehr die Realität, die Software präsentiert vielmehr eine vorselektierte Realität. Somit wird durch die Software bereits bestimmt, welche Situationen überhaupt in den Aufmerksamkeitsbereich der Polizei geraten.

Grenzfälle der Mustererkennung

Ohne Zweifel sind mit den Verhaltensscannern schwerwiegende Eingriffe in die Persönlichkeitsrechte und in weitere Grundrechte der Vorbeiläufenden verbunden. Um die Eingriffstiefe zu bestimmen, muss man fragen, wie viele eigentlich polizeilich nicht relevante Situationen der Verhaltensscanner als gefährlich markiert. Dieser Punkt wird bei einer permanenten automatisierten Beobachtung

essentiell, weil schon eine relativ kleine Fehlalarmquote bei vielen beobachteten Situationen eine große Zahl falscher Treffer erzeugen kann. Diese wiederum erzeugen Zumutungen für diejenigen Menschen, deren Tagesabläufe in den Bereich der Grenzfälle einer Mustererkennung fallen und zu Diskriminierungen führen können. Dazu gehören beispielsweise Menschen, die aufgrund von physischer oder psychischer Konstitution oder durch Behinderungen abweichendes Verhalten zeigen.

Nach Satz 3 dieser Vorschrift sollen auch Menschen in den als alarmierend ausgewiesenen Situationsaufnahmen speziell markiert werden dürfen, wenn ein Beschäftigter der Polizei dies veranlasst. Dadurch soll eine „automatisierte Nachverfolgung“ angestoßen werden.

Diesen Ablauf sollte man sich verdeutlichen im Lichte der Gefahr, dass in jedem dieser Schritte Fehler passieren können, die zu Folgefehlern in jedem der nächsten Schritte führen:

- 1) Erkennung eines trainierten Musters durch die Scanner-Software,
- 2) Markierung der Situation,
- 3) Auswahl einer Person,
- 4) automatisierte Nachverfolgung dieser Person,
- 5) gegebenenfalls Identifizierung.

Markiert der Verhaltensscanner beispielsweise die falsche Person mit dem Stigma „auffälliges Bewegungsmuster“, verfolgt das System anschließend diese falsche Person über weitere Kameras und könnte dabei mehr scheinbare Auffälligkeiten erkennen. Dann wird aus einem einzelnen Fehlalarm eine ganze Kette scheinbar zusammenhängender Beobachtungen.

Die Wiedererkennung einer markierten Person während der Nachverfolgung darf auch über ein biometrisches Merkmal erfolgen, also etwa Körpermerkmale des betroffenen Menschen wie Gesicht, Stimme oder Gang. Auch andere technische Möglichkeiten ohne Biometrieinsatz sind möglich, etwa über mitgeführte Taschen, Fahrräder oder getragene Kleidung.

Laut Gesetzentwurf sollen jedoch „vorrangig nicht körperliche Merkmale“ verwendet werden. Damit bleibt biometrische Erkennung allerdings immer möglich, darf aber (vorerst) nicht zur biometrischen Fernidentifikation zweitgenutzt werden.

3. Biometrische Fernidentifikation

Der Entwurf sieht die Nutzung biometrischer Erkennungstechnologien im öffentlichen Raum in automatisierter Form vor. Vereinfacht gesagt soll der Polizei erlaubt werden, Menschen mit Hilfe derjenigen vorliegenden Aufnahmen direkt zu identifizieren, aus denen biometrische Merkmale extrahiert wurden.

Der Gesetzentwurf sieht in § 184b und § 184c konkret vor, dass von der Polizei erstellte Fotos, Audio- oder Videoaufnahmen von Menschen bei öffentlichen Veranstaltungen und Ansammlungen und an allgemein zugänglichen Orten künftig unter bestimmten Bedingungen weiterverwendet werden dürfen. Das soll

bereits unter minimalen Voraussetzungen erlaubt werden: Es dürfen dann aus dem Fotomaterial die biometrischen Merkmale der Abgebildeten extrahiert und zur Identifizierung genutzt werden.

Als biometrische Merkmale gelten diejenigen biologischen, physiologischen und verhaltensbezogenen Merkmale eines Menschen, aus denen sich unterscheidbare, gut wiederholbare und möglichst langzeitstabile Merkmale zur Identifizierung ableiten lassen. Verbreitet ist die Nutzung von Fingerabdrücken, Gesichtern, Tastaturanschlägen, Stimmen und Iriden. Biometrischen Technologien wohnt ein hohes Diskriminierungspotential inne, insbesondere für ethnische Minderheiten, Senioren und Frauen.

Biometrische Daten gehören zu den besonders sensiblen personenbezogenen Daten und genießen in Europa einen verstärkten Schutz. Ihre Verarbeitung bedarf deshalb einer besonders tragfähigen gesetzlichen Grundlage und strenger Verhältnismäßigkeitsanforderungen. Sie muss durch Grundrechtsgarantien für die Betroffenen flankiert werden. Ob es eine Erforderlichkeit und Notwendigkeit der Biometrienutzung überhaupt geben kann im Bereich der Gefahrenabwehr, also bevor etwas passiert ist oder auch nur ein Verdacht auf eine konkrete Straftat besteht, ist bereits fraglich.

Bei heute verfügbaren Biometriesystemen ist typischerweise an Gesichtsmerkmale zu denken. Je nach Art des Ausgangsmaterials kommen aber auch andere biometrische Merkmale in Betracht, im Entwurf wird deren Art nicht beschränkt. Die Eingriffsintensität entsteht hier nicht erst bei der Identifizierung, sondern bereits durch die automatisierte Umwandlung von Bild- oder Tonaufnahmen in biometrisch auswertbare Daten.

Die technische Weiterverarbeitung soll „automatisiert in Echtzeit“ erfolgen. Das Ziel ist, die Identität erkennbarer Personen auf den Bildern von öffentlichen Veranstaltungen und Ansammlungen und von allgemein zugänglichen Orten anhand von deren Körpermerkmalen zu verifizieren. Dazu müssen aus den Abbildungen oder Audio- oder Videoaufnahmen diese biometrischen Merkmale zunächst gewonnen und technisch umgewandelt und gespeichert werden, um sie danach als „biometrische Referenzdaten“ verwenden zu können.

Diese biometrischen Datensätze sollen dann „mittels einer automatisierten Anwendung zur Datenverarbeitung in Echtzeit“ mit anderen biometrischen Daten verglichen werden.

Hinzu tritt im Entwurf die neue Befugnis des § 195b, wonach der biometrische Abgleich unter bestimmten Bedingungen auch mit „in öffentlich zugänglichen Daten des Internet erkennbaren Personen“ erlaubt wird. Das darf „automatisiert“ erfolgen.

Dazu müssen wiederum zunächst aus diesen öffentlichen Daten des Internet biometrische Referenzdaten gewonnen werden, um technisch den Abgleich durchführen zu können. Das kann nicht ohne eine Datenbank erfolgen, in der die verfügbaren Bilder aus dem Internet für den Abgleich durchsuchbar vorgehalten werden. Technisch ist das nicht anders umsetzbar, da ein Echtzeit-Abgleich an der Notwendigkeit der vorherigen Referenzdatenerzeugung scheitert und damit praktisch nicht möglich ist.

Keine Anonymität mehr in der Öffentlichkeit

Praktisch gesprochen bedeutet die neue Befugnis aus Sicht von Menschen, die an öffentlichen Veranstaltungen und Ansammlungen teilnehmen: Jedes öffentlich zugängliche Foto oder Video, aus dem ein biometrisches Merkmal wie das Gesicht oder die Stimme extrahiert werden kann, darf nun zu einem polizeilich nutzbaren Identifikationsobjekt umfunktioniert werden. Wegen der heutigen Omnipräsenz von Geräten, die Fotos und Videos machen können, gerieten wir damit in eine Situation, die Anonymität in der Öffentlichkeit faktisch nicht mehr zuließe.

Qualitativ stark beschränkt ist im Entwurf weder die Art der nutzbaren öffentlich zugänglichen Daten noch die Art der biometrischen Merkmale. Lediglich zwei Einschränkungen sind enthalten.

Erstens soll der biometrische Abgleich nicht mit Daten erfolgen, „die aus im Internet in Echtzeit übertragenen und veröffentlichten Video-, Audio- oder Bilddateien gewonnen werden“. Damit könnten etwa Live-Streams gemeint sein. Diese Einschränkung ist praktisch fragwürdig, da Aufzeichnungen von Streams heute gängig sind.

Zweitens soll bei den Daten aus dem Netz die Intimsphäre der Menschen beachtet werden, es soll also nicht in den besonders geschützten Kernbereich privater Lebensgestaltung eingegriffen werden. Beim Kernbereich ist es wegen des absoluten Schutzes notwendig, schon die Möglichkeit auszuschließen, dass höchstpersönliche Daten verwendet werden.

Auch bei Gefahrenabwehrinstrumenten im Polizeirecht darf nicht in diesen Kernbereich eingedrungen werden, wie das Bundesverfassungsgericht vielfach betont hat.² Dass beim automatisierten Abgrasen des Internet nach erkennbaren Personen auch höchstpersönliche Aufnahmen eingesammelt werden könnten, ist möglich. Daher müssen gesetzliche Schutzvorkehrungen eingebaut werden, die aber praktisch an Anwendungsschwierigkeiten stoßen. Da bisher keine Aufnahmen von Menschen automatisiert und damit massenhaft ausgewertet werden, um daraus biometrische Referenzdaten zu erzeugen, sind keine Verfahren für den Kernbereichsschutz solcher Massensammlungen etabliert.

Nachträglicher Abgleich

Welchen Sinn eine spezielle Regelung zur Zeitverzögerung bei der Nutzung der biometrischen Merkmale haben soll, erschließt sich nicht. Wer einen biometrischen Abgleich als „nachträglich“ definiert, müsste eine Zeitspanne angeben und das Ereignis nennen, ab dem diese Spanne beginnt.

Es drängt sich auf, dass die Logik dahinter nur dem Wunsch entspringt, diese biometrischen Abgleiche nach Art. 5 KI-Verordnung überhaupt gangbar zu machen. Wenn aber die rechtliche Zulässigkeit davon abhängt, ob ein System als Echtzeit- oder als nachträgliche Fernidentifizierung eingestuft wird, darf nicht bereits eine geringe oder künstlich erzeugte Verzögerung zu einer Umgehung der strengeren Anforderungen führen.

² Vgl. „unantastbarer Kernbereich privater Lebensgestaltung“, in BVerfGE 109: 279ff., BVerfGE 100: 313ff.

Schließlich ist die KI-Verordnung keineswegs ein Freibrief für den Einsatz von Gesichtserkennung im Rahmen der Gefahrenabwehr, sondern spannt den äußersten Rahmen für eine gerade noch akzeptable Verwendung auf. Diesen Rahmen nicht nur auszuschöpfen, sondern noch mit einer Technizität zu unterlaufen, ist nicht mehr tragbar. „Menschliche Kontrolle“ ist unionsrechtlich kein optionales Feigenblatt, sondern Teil der Schutzarchitektur. Im Gesetzentwurf ist diese Schutzarchitektur nicht wirksam und nachvollziehbar in Landesrecht übersetzt.

Eine nachträgliche Fernidentifizierung ist dabei nicht weniger eingriffsintensiv: Auch hier werden Körpermerkmale zur Identifikation verwendet, um einen für die Betroffenen heimlichen Abgleich mit öffentlich zugänglichen Informationen zu vollziehen.

Sowohl im Falle von § 184b als auch § 195b soll der Biometrieabgleich den Vorgaben der KI-Verordnung genügen. Dazu soll das Ergebnis eines Abgleichs jeweils „durch zwei qualifizierte Beschäftigte der Polizei“ geprüft werden. Falls danach polizeiliche Maßnahmen erfolgen, soll der gesamte biometrische Datensatz (mit allen Daten des Abgleichs) gespeichert werden dürfen. Im Falle des nachträglichen Biometrieabgleichs sollen auch alle weiteren erlangten personenbezogenen Daten mitgespeichert werden. Andernfalls sollen sie gelöscht werden.

Biometrische Massenüberwachung

Ob auch kommerzielle Gesichtserkennungsdatenbanken und private Anbieter durch die Polizei genutzt werden könnten, lässt der Entwurf offen. Solche Anbieter sammeln Fotos aus dem Internet ein und erstellen damit eine durchsuchbare Datenbank aus Milliarden biometrischer Merkmale der Gesichter. Die Praxis ist in Europa rechtswidrig, wird aber seit Jahren faktisch geduldet.

Die geplanten biometrischen Erkennungstechnologien zur Identifizierung betreffen besonders viele Unbeteiligte und verarbeiten zudem massenhaft besonders geschützte Körperdaten.

Der Chaos Computer Club setzt sich für ein eindeutiges Verbot biometrischer Fernidentifikationssysteme ein. Die Vorhaben sind aus dem Entwurf zu streichen und stattdessen Maßnahmen zu ergreifen, um Menschen wirksam vor Software-gestützter Gesichtsrasterung und Massenüberwachung zu schützen.

Neue Befugnisse zusammen betrachtet

Jede einzelne dieser neuen Befugnisse lässt sich im Prinzip einschränken: öffentliche Beobachtung, automatisierte Mustererkennung, Identifizierung, Abgleich mit Polizeidaten, automatisierte Datenanalyse, automatisierte Erzeugung neuer Zusammenhänge oder Erkenntnisse und die resultierende polizeiliche Gefahrenprognose. Höchst problematisch ist jedoch die Möglichkeit ihrer Verkettung.

Schon die einzelnen Maßnahmen sind jeweils in hohem Maße eingriffsintensiv. Zusammengenommen entsteht ein sehr mächtiges und gefährliches System.

Das Bundesverfassungsgericht hat bereits bei der automatisierten Datenanalyse vor einer daten- und methodenoffenen Ausgestaltung der Regelungen ausdrücklich gewarnt. Denn die Polizei kann mit diesen neuen Kompetenzen aus großen Datenmengen neue Verdachtszusammenhänge generieren und so eine ständige Rasterfahndung auf weiten Teilen der Bevölkerung umsetzen.

Eine ursprünglich wegen des personellen Aufwands nur selektiv umsetzbare Überwachung durch die Polizei wird durch den neuen datengetriebenen Ansatz skalierbar. Dies begründet ein eigenständiges rechtsstaatliches Risiko. Denn es werden neue technische und organisatorische Infrastrukturen etabliert, die nicht nur getrennt betrachtet werden dürfen: Videokameras im öffentlichen Raum, permanente Bewegungsmustererkennung, Erstellung massenhafter biometrischer Referenzdaten, automatisierte Datenanalyse mit der Zusammenführung der Polizeidaten und damit einhergehende Such- und Profilbildungsmöglichkeiten. Die Anwendungsbereiche könnten künftig auch ohne einen grundlegenden technischen Umbau erheblich erweitert werden – nur durch die Änderung der Zwecke, Schwellenwerte oder Analysekriterien.

Gerade deshalb muss der Gesetzentwurf die Befugnisse bereits ausreichend begrenzen, damit Missbrauchsmöglichkeiten nicht durch eine spätere Änderung der Anwendungspraxis ausgeweitet werden können. Wir empfehlen daher eine Reihe von Korrekturen:

- statt einer Verlagerung in Verwaltungsvorschriften: gesetzliche Regelung zur wesentlichen Begrenzungen von Art und Umfang der verarbeitbaren Daten, der zulässigen Analysemethoden und des Automatisierungsgrades,
- verpflichtende unabhängige technische und datenschutzrechtliche Audits, einschließlich Fehlerraten, Datenqualität und möglichen diskriminierenden Auswirkungen,
- verpflichtende unabhängige wissenschaftliche Evaluation der tatsächlichen Wirksamkeit und Erforderlichkeit der neuen Befugnisse,
- regelmäßige öffentliche Transparenzberichte über Anzahl und Anlass der Einsätze, Zahl der automatisierten Treffer, Fehllalarme, nachfolgende polizeiliche Maßnahmen und deren Ergebnisse, nachvollziehbare Dokumentation der automatisierten Vorbewertungen,
- strikte technische Begrenzung der Einbeziehung externer Datenquellen,
- keine selbstlernenden Systeme.

Fazit

Die vorgeschlagenen Befugnisse erweitern nicht einfach einzelne polizeiliche Instrumente, sondern schaffen eine neue Infrastruktur, in der Beobachtung, automatisierte Mustererkennung, biometrische Identifizierung und viele bisher getrennte Datenbestände miteinander verknüpft werden können. Diese Verknüpfung ist teilweise dauerhaft.

Jede dieser Technologien kann einen Nutzen haben. Ein zentrales Risiko entsteht jedoch dann, wenn automatisierte Systeme aus unvollständigen oder bereits verzerrten Daten scheinbar belastbare Zusammenhänge erzeugen. Diese Zusammenhänge können die Auswahl polizeilicher Maßnahmen beeinflussen und daraus entstehende neue Daten können wiederum in weitere Analysen einfließen. Fehler, Verzerrungen und diskriminierende Effekte werden dadurch nicht erkannt, sondern können – im Gegenteil – verstärkt werden.

Es ist erforderlich, die skizzierten gesetzlichen Begrenzungen, unabhängige Kontrollen, Transparenz- und Evaluationspflichten sowie die Begrenzung des Automatisierungsgrads bereits im Gesetz selbst zu verankern. Nur so lässt sich sicherstellen, dass der Einsatz neuer Polizeitechnik nicht durch seine eigene Leistungsfähigkeit zu einem kaum noch oder gar nicht mehr kontrollierbaren Eingriffsinstrument wird.

Der Gesetzentwurf enthält weitere Überwachungsmaßnahmen technischer und nicht-technischer Natur. Die vom Bundesverfassungsgericht angeregte Gesamtüberwachungsrechnung ist daher überfällig.