



Ausschussdrucksache 21(4)214 H
vom 21. September 2026

Schriftliche Stellungnahme

von Hadmut Danisch vom 21.9.2026

zu dem

- a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus
BT-Drucksachen 21/6131, 21/7265
- b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksachen 21/6132, 21/6511
- c) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen
BT-Drucksache 21/6806
- d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten
BT-Drucksache 21/6913
- e) Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, weiterer Abgeordneter und der Fraktion Die Linke
Nein zu biometrischen Massenerkennungssystemen
BT-Drucksache 21/6917

Stellungnahme als Sachverständiger

für den Deutschen Bundestag

zum

- a) Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“, BT-Drucksachen 21/6131, 21/7265**
- b) Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“, BT-Drucksachen 21/6132, 21/6511**
- c) Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“, BT-Drucksache 21/6806**
- d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN „Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten“, BT-Drucksache 21/6913**
- e) Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, weiterer Abgeordneter und der Fraktion Die Linke „Nein zu biometrischen Massenerkennungssystemen“, BT-Drucksache 21/6917**

Anhörung am 21. September 2026
– Innenausschuss (41. Sitzung) –

Dipl.-Inform. Hadmut Danisch

Stand: 21. September 2026

(Dokumentlinks blau, externe Links rot)

Inhaltsverzeichnis

1	Formale Angaben	5
1.1	Auftrag	5
1.2	Gegenstand	5
1.3	Unzureichende Bearbeitungszeit	6
1.4	Maßstab	7
1.5	Sachkunde	9
I	Antrag der Bundesregierung zur Strafprozessordnung (21/6806)	10
2	Unklarheiten, Fehler, Inkonsistenzen	11
2.1	Regelungsgehalt und Neuigkeitswert	11
2.2	Diskrepanz zwischen Begründung und Inhalt	12
2.3	Formulierung „Aus einem Strafverfahren“	13
2.4	Begriff der „öffentlich zugänglichen Daten aus dem Internet“	15
2.4.1	„aus dem Internet“	15
2.4.2	„öffentlich zugänglich“	15
2.4.3	Jugendsperre	16
2.5	Begriff der „biometrischen Daten“	16
2.6	Begriff der „Echtzeitdaten“	19
2.7	Reichweite des beantragten § 98d StPO	21
2.7.1	Beispiel: Ehefrau	21
2.7.2	Beispiel: Klette/Garweg	21
2.7.3	Beispiel: Kinderpornographie	22
2.7.4	Beispiel: Wohnzimmerschrankwand	22
2.8	Wieviel darf an die KI ausgelagert werden (Art. 33 Abs. 4 GG)?	23
2.9	Berufsgeheimnisse und Zeugnisverweigerungsrechte	23
2.9.1	Tracking von Verweigerungsberechtigten	23
2.9.2	Ausweitung der Verstrickungsklausel	24
2.9.3	Ausdehnung der StPO	26
2.10	Misgendern	26
2.11	Datenschutz: Besondere Kategorien personenbezogener Daten	27
2.12	Indirekter Nutzen?	28
2.13	„Spieglein, Spieglein an der Wand, wer ist die Schönste im ganzen Land?“	29
2.14	Datenflut der USA	31
2.15	Beweislast?	32
2.16	Haftung?	32
2.17	Evaluierung?	33

3	Beeinträchtigte Grundrechte	34
3.1	Rechtswegsgarantie (Art. 19 Abs. 4 GG)	34
3.2	Meinungsfreiheit (Art. 5 Abs. 1 GG)	34
3.3	Pressefreiheit (Art. 5 Abs. 1 GG)	35
3.4	Versammlungsfreiheit (Art. 8 GG)	35
4	Verhältnismäßigkeit	36
4.1	„auch im Einzelfall erhebliche Bedeutung“	36
4.2	Fehlende Voraussetzung schuldhaften Verhaltens	36
5	Missbrauch	38
5.1	Missbrauch von innen	38
5.1.1	Politischer Missbrauch	38
5.1.2	Unterwanderung durch organisierte Kriminalität	38
5.1.3	Unterwanderung durch Linksextremismus	39
5.1.4	Akteneinsicht	40
5.2	Fälschung und Täuschung von außen	41
5.3	Naive Sicht auf Aufsichtsbehörden	42
II	Antrag der Bundesregierung zur Polizeiarbeit (21/6132)	45
6	Unklarheiten, Fehler, Inkonsistenzen	46
6.1	Bezugnahme auf die StPO-Kritik	46
6.2	Datenaustausch mit Drittstaaten	46
6.3	Diskrepanz zwischen § 9a und § 9b BKAG	46
6.4	Selbstlernende Systeme	47
6.5	Auslagerung in die USA?	47
6.6	Richtervorbehalt	48
6.7	„diskriminierende Algorithmen“	48
6.8	§ 15b verunglückt	48
6.9	Falscher Begriff der Gewährleistung	48
7	Verhältnismäßigkeit	50
7.1	Bezugnahme auf die StPO-Kritik	50
III	Antrag der Bundesregierung zur Terrorismusabwehr (21/6131)	51
8	Unklarheiten, Fehler, Inkonsistenzen	52
8.1	Bezugnahme auf die StPO- und Polizei-Kritik	52
8.2	Sicherung von Verkehrsdaten	52
8.2.1	Thematische Zuordnung	52
8.2.2	Zeitpunkt	52
8.2.3	Was sind „Verkehrsdaten“?	53

IV	Gegenanträge	54
9	Antrag der Grünen (21/6913)	55
9.1	Kommentar statt Antrag	55
9.2	Leeres Blabla	55
9.3	„Algorithmen“	55
9.4	Keine Stellungnahme	56
10	Antrag der Linken (21/6917)	57
10.1	Positionierung statt Antrag	57
10.2	Politische Absichten	58
10.2.1	RAF und linker Terror	58
10.2.2	Migration und Islamischer Staat	59
10.3	Wertung	59
V	Ergebnis	61
11	Regierungsanträge	62
11.1	Gesamtergebnis	62
11.2	Ergänzende Begründungen	63
11.2.1	Position zur Biometrie	63
11.2.2	Keine ausreichende Diskussion	64
11.2.3	Angreifbarkeit vor dem Bundesverfassungsgericht	65
11.2.4	Mangelnde Sachkunde	66

1 Formale Angaben

1.1 Auftrag

Ich wurde am 17.9.2026 vom Innenausschuss des Deutschen Bundestages zur Stellungnahme zu den und zur Teilnahme an der öffentlichen Anhörung über die nachfolgend unter Gegenstand aufgelisteten Anträge eingeladen.

Eine explizite Frage- oder Problemstellung gab es nicht. Die Stellungnahme erfolgt deshalb als freie Äußerung.

1.2 Gegenstand

Gegenstand der Betrachtung sind:

BT-Drucksachen 21/6131 und 21/7265: Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“ und Stellungnahme des Bundesrates

BT-Drucksachen 21/6132 und 21/6511: Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ und Stellungnahme des Bundesrates

BT-Drucksache 21/6806: Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“

BT-Drucksache 21/6913: Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, Marcel Emmerich, Jeanne Dillschneider, Rebecca Lenhard, Helge Limburg, Filiz Polat, Lukas Benner, Schahina Gambir und der Fraktion BÜNDNIS 90/DIE GRÜNEN „Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten“

BT-Drucksache 21/6917: Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, Anne-Mieke Bremer, Katrin Fey, Dr. Gregor Gysi, Ferat Koçak, Jan Köstering, Sonja Lemke, Bodo Ramelow, David Schliesing, Aaron Valent, Christin Willnat und der Fraktion Die Linke „Nein zu biometrischen Massenerkennungssystemen“

Ferner wurden herangezogen

- Die **Strafprozessordnung**
- Das **Bundeskriminalamtgesetz**
- **DSGVO** und **BDSG**
- BVerfG 1 BvR 1547/19, 1 BvR 2634/20 („Automatisierte Datenanalyse“)

Weitere Quellen – wie Rückfragen bei den Antragstellern oder bestehende Rechtsprechung – konnten in der Kürze der zur Verfügung stehenden Zeit nicht eingeholt werden.

1.3 Unzureichende Bearbeitungszeit

Die Beauftragung erfolgte so kurzfristig, dass mir zur Bearbeitung und Erstellung der vorliegenden Stellungnahme effektiv nur zweieinhalb Tage über das Wochenende zur Verfügung standen. Diese Zeit reichte nicht aus,

- um die Materie samt aller Querverweise völlig zu durchdringen,
- Rechts- und Literaturrecherche zu betreiben,
- Rückfragen an die Antragsteller zu stellen (die aus meiner Erfahrung früherer Stellungnahmen für Bundestag und Landtage aber ohnehin nicht beantwortet werden¹),
- vollständig nach Fehlern und rechtsstaatlichen Problemen zu suchen,
- die – insbesondere in 21/6806 genannten – EU-Verordnungen oder Urteile nachzuverfolgen,
- mir eine abschließende Meinung zu bilden,
- eine Ausarbeitung in der von mir angestrebten Qualität und Tiefe auszuarbeiten,
- eine mündliche Stellungnahme auszuarbeiten und vorzubereiten.

Die vorliegende Stellungnahme erhebt daher keinen Anspruch auf Vollständigkeit.

Etwaige Schreibfehler, Grammatikfehler, holprige Formulierungen, Wiederholungen usw. bitte ich daher zu entschuldigen. Die Stellungnahme wurde unter hohem Zeitdruck erstellt. Ich werde bei Bedarf eine korrigierte Version nachreichen.

¹An dieser Stelle möchte ich beim Bundestag anregen, nicht nur die Sachverständigen darüber zu belehren, dass sie gehalten sind, in der Anhörung Fragen aller Fraktionen zu beantworten, sondern umgekehrt und auf Gegenseitigkeit auch die Regierung und die Fraktionen in derselben Weise anzuhalten, Fragen der Sachverständigen zu beantworten.

1.4 Maßstab

In der Kürze der zur Verfügung stehenden Zeit war es nicht möglich, einen formalen und explizit ausformulierten Maßstab zu finden oder bilden und anzuwenden.

Ich lege deshalb als Maßstab meine Berufs-, Praxis- und Lebenserfahrung im Bereich der IT-Sicherheit, der Vorratsdatenspeicherung, des Datenschutz- und Verwaltungsrechts, und als Blogger² zu solchen Themen an.

Insbesondere erfolgt meine Stellungnahme unter dem Eindruck und damit selbstverständlich auch unter dessen Anwendung als Maßstab

- eines Strafermittlungsverfahrens, das unter dem Vorwand des § 188 StGB und dem Vorhalt, ich hätte eine grüne Politikerin beleidigt, weil ich mich zu einer Pressekampagne, zu ihrem Wahlkampf und zu ihrem Erscheinungsbild kritisch geäußert hatte, geführt wurde, und bei dem sich herausstellte, dass es nur als Tarnung diene, um heimlich eine unrechtmäßige Kontenabfrage und Kontenkündigung zu betreiben, wie von der damaligen Bundesinnenministerin Nancy Faeser öffentlich angekündigt, nachdem ich als Blogger zuerst Unstimmigkeiten im Lebenslauf der damaligen Kanzlerbewerberin Annalena Baerbock gefunden hatte, und die Grünen gegenüber dem Verfassungsschutz behaupteten, dass wegen Nordstream 2 mit den Russen unter einer Decke stecken müsse, wer Annalena Baerbock kritisiere,
- einer missbräuchlichen Betriebsprüfung, die das Finanzamt unter – unwahren, vorgeschobenen und rechtsfehlerhaften – Vorwänden für genau denselben Zeitraum bei mir anordnete, nachdem die Staatsanwaltschaft den erhofften Russenauftrag bei mir nicht fand, und deren einziges erkennbares Ziel war, weitere Konten in diesem Zeitraum zu durchsuchen, und damit fraglos eine Tätigkeit für den Verfassungsschutz war (zu dessen Unterstützung in Berlin auch die Finanzämter gesetzlich verpflichtet sind),
- eines Zivilrechtsstreites, den ich gerade hinter mir habe, der nur vorgeblich im Namen einer Grünenpolitikerin erfolgte, tatsächlich aber von HateAid betrieben wurde, die ich für eine regierungsnah Tarnorganisation halte, um verfassungswidriges Regierungshandeln in das Privatrecht auszulagern, und dabei haarsträubende Vorgänge am Landgericht, am Kammergericht und am Bundesverfassungsgericht erlebt habe.

Dazu kommen eine Vielzahl von – weitgehend vertraulichen – Hinweisen von Lesern meines Blogs, die darauf schließen lassen, dass die Regierung in großem Umfang und sehr weitgehend die Staatsgewalt zum Zwecke politischer Agitation und des Machterhalts missbraucht.

Dazu kommen weitere persönliche Erfahrungen mit massiven – rechtswidrigen und

²20 Jahre, 30.000 Blogartikel

missbräuchlichen – Eingriffen der jeweiligen Regierung oder Regierungsfractionen in das Verwaltungs- und Zivilrecht in den Jahren 1998 bis 2007, 2009 und 2012.

Ich hatte in zwei Bereichen beruflich jeweils mehrmals mit dem Bundeskriminalamt und dessen „Ermittlungsmethoden“ zu tun, bei der Vorratsdatenspeicherung und bei der Kinderpornosperre (beides 2009). Ich stehe dem Bundeskriminalamt seither kritisch gegenüber, und halte es nicht für seriös – zumindest nicht hinreichend für seine Aufgaben.

Ich betrachte daher solche Fragestellungen – gewollt und ungewollt – immer

- aus der Sicht des Informatikers unter technischen Aspekten und in Bezug auf Massenanzwendung,
- aus meiner persönlichen Erfahrungen unter dem Aspekt des staatlichen Missbrauchs und Rechtsbruchs durch die – politisch gesteuerte und missbrauchte – Justiz.

Damit liegt eine Art impliziten Maßstabs vor.

1.5 Sachkunde

- 1994 Diplom in Informatik
- über 35 Jahre hauptberufliche Tätigkeit als Informatiker, davon 10 Jahre in Forschung und Lehre zu IT-Sicherheit und Kryptographie, 23 Jahre in der Industrie als IT-Sicherheitsexperte, Information Security Officer, Datenschutzkoordinator, Compliance Officer
- davon 7 Jahre bei Internet-Providern
- 9 Jahre im Post- und Fernmeldebereich
- Mitarbeit am Aufbau des Internet in Deutschlands, u.a. Absicherung und Anschluss des ersten Kernkraftwerks an das Internet, mehrfach sicherheitsüberprüft
- **3 Jahre in der Rechtsabteilung eines großen Telefon- und Internetanbieters in Deutschland**
- **dabei 1 Jahr (2009) in der Vorratsdatenspeicherung und Beauskunftung, Aufsicht und Eingangsprüfung von zwischen 1.000 und 2.000 Fällen**
- **2009 als Vertreter eines Telefon- und Internetanbieters am Vorhaben der Kinderpornosperr der Regierung (Ursula von der Leyen) involviert. Die Sperre wurde durch das BKA abgeblasen, nachdem ich das BKA beraten und die Fehler und Probleme im Vorhaben aufgezeigt habe.**
- 1997 Assistent und Ghostwriter bei Anhörung zum Kryptographieverbot des Deutschen Bundestags
- 1998 Gutachten „Künftige Anforderungen an die Kommunikationssicherheit in der Medizin“ für den Deutschen Bundestag (BT-Ds 13/11002)
- 2019 Stellungnahme zu „Uploadfiltern“, Anhörung im Abgeordnetenhaus Berlin
- 2020 Stellungnahme zur Erhöhung der Rundfunkbeiträge, Anhörung im Landtag Sachsen
- 2021 Stellungnahme zum MDR Staatsvertrag, Anhörung im Landtag Thüringen
- 2023 Stellungnahme für den Bundestag zur Vorratsdatenspeicherung
- Über 30.000 Blogartikel zu Rechts- und Medienpolitik und vielen anderen Themen

Teil I

Antrag der Bundesregierung zur Strafprozessordnung (21/6806)

2 Unklarheiten, Fehler, Inkonsistenzen

2.1 Regelungsgehalt und Neuigkeitswert

Auf den *ersten* Blick erscheint fraglich, welchem Zweck diese Gesetze dienen, denn bisher schon gilt nach § 161 Abs. 1 Satz 1 StPO gilt

Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und **Ermittlungen jeder Art** entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

Es hört sich an, als sage man „*bisher durften wir schon alles, aber das reicht uns nicht, wir brauchen noch mehr Befugnisse!*“

Auch erscheint der Einsatz von Biometrie nicht neu denn schon lange verwendet man Biometrie als Fahndungsmittel,

- Größe, Haarfarbe, Augenfarbe, Aussehen, Foto, Phantombild, Tätowierungen, Narben, fehlende Körperteile, sind schon lange Fahndungsmittel und waren im 19. Jahrhundert bereits polizeiüblich.

In den 70er Jahren war alles mit Fahndungsplakaten der RAF tapeziert, überall hingen – *effektiv biometrische* – Fahndungsfotos und Personenbeschreibungen auf dem damaligen Stand der Technik.

- Fingerabdrücke waren das große biometrische Ding des 20. Jahrhunderts.
- DNA, Augenerkennung (Iris oder Netzhaut) und andere, computergestützte biometrische Verfahren (z. B. Venenerkennung) sind die biometrischen Verfahren des frühen 21. Jahrhunderts.

Wo ist der Neuigkeitswert?

Formal geht es darum, den Wünschen des Bundesverfassungsgericht nach ausdrücklicher gesetzlicher Grundlage und Regelung nachzukommen, also eher eine implizit bereits bestehende Rechtslage explizit zu bekräftigen.

Liest man das Kleingedruckte, dann geht es um Massendatenverarbeitung und den Einsatz von KI und ausländische Dienste – die Biometrie ist nur das Neben- und Marketingthema. Nach der Festnahme von Daniela Klette fragten viele, warum ein Kanadischer Journalist sie innerhalb von 30 Minuten finden konnte, indem er ein altes

RAF-Fahndungsfoto in die KI-basierte Gesichtserkennungssoftware PimEyes eingab und damit ein Foto aus ihrem Capoeira-Kurs fand (Quelle: [Verfassungsblog](#)).

Es geht also nicht einfach nur um die Anwendung biometrischer Techniken, sondern die Massenauswertung praktisch des gesamten öffentlichen Lebens, das heute längst in Form von Texten, Fotos, Videos im Internet stattfindet, als Fahndungsmaßnahme.

Vergleicht man das damit, welchen großen öffentlichen Diskussionen und Reaktionen es damals in den 1970ern zur Rasterfahndung und den 1980ern zur Volkszählung gab, erscheint mir die Unauffälligkeit und das fehlende Medienecho zu diesem Gesetz, das sehr viel weiter geht als Rasterfahndung und Volkszählung, grotesk.

Vor 30, 40 Jahren hätte man den Bundestag mit Demonstrationen dafür mindestens lahmgelegt, über ein solches Gesetz auch nur nachzudenken. Es erscheint seltsam, wie wenig Beachtung diese Gesetzentwürfe heute finden, was dafür spricht, dass viele sie einfach nicht verstehen – und sie womöglich bewusst unklar gehalten sind.

Es erscheint mir deshalb wichtig zu betonen, dass zwar der Aspekt und der Begriff der Biometrie hier dominant sind und die Aufmerksamkeit an sich ziehen, der wichtigere Aspekt aber die

- massenhafte Erfassung von Daten aus dem frei zugänglichen Internet, insbesondere Social Media, Blogs, Podcasts, Youtube, TikTok, Instagram usw. ist,
- deren massenhafte Erkennung und Auswertung durch KI,
- die Zusammenführung von Daten,
- die Nutzung ausländischer Dienstleister

und damit eine nicht nur enorme, sondern totale Datenerfassung aller Bürger ist. Wer heute Kind oder noch Jugendlicher ist, dessen gesamtes modernes Leben kann damit erfasst werden. Und dessen gesamter Lebenslauf zum Gegenstand strafrechtlicher Ermittlungen wird.

Das alles wird über die Biometrie überdeckt, und fährt damit im Windschatten der Causa Daniela Klette, die für eine Grundakzeptanz biometrischer Fahndung gesorgt hat.

2.2 Diskrepanz zwischen Begründung und Inhalt

Der Regelungsbedarf wird – über die drei Entwürfe verteilt – mit der Gefahr durch

- terroristische Organisationen wie den „Islamischen Staat“
- Linksextremismus

- internationale Konflikte etwa im Nahen und Mittleren Osten
- schwere Gewalttaten durch Einzeltäter im öffentlichen Raum

begründet, was – unbestritten – schwere Bedrohungen des Staates und der öffentlichen Sicherheit sind, und denen entgegenzutreten Kernaufgabe des Staates ist.

Dem Wortlaut und der praktischen Auslegung nach gelten die Ermittlungsmaßnahmen aber schon

- bei kleinsten Bagatellen wie der Äußerungen, die als Beleidigung nach § 188 StGB ausgelegt werden,
- Strafverfahren, die wegen Unschuld eingestellt werden,
- für Zeugen
- für unbeteiligte Dritte, wenn deren Aufenthaltsort Aufschluss geben kann.

Die Begründung trägt den tatsächlichen Regelungsgehalt nicht, weil dieser weit über die Begründung hinaus geht.

2.3 Formulierung „Aus einem Strafverfahren“

Der beantragte neue § 98d StPO enthält die Formulierung

... dürfen biometrische Daten aus einem Strafverfahren ...

Der Begriff des Strafverfahrens wird zwar auch in den bereits bestehenden Gesetzen oft verwendet, **ist aber nirgends definiert**. Die Strafprozessordnung kennt drei Verfahrensabschnitte,

- das Vorverfahren
- das Zwischenverfahren
- das Hauptverfahren

Dazu kommt noch die Phase zwischen Anzeigeerstattung und Entschließung der Staatsanwaltschaft über die Aufnahme von Ermittlungen.

Es bleibt unklar, ob hier auch biometrische Daten aus einem Anzeige- oder Vorverfahren gemeint sind, wenn etwa die Staatsanwaltschaft keine Anklage erhebt, weil sich der Verdacht nicht erhärtet, oder das Gericht die Anklage nicht zulässt.

Damit sind dann auch Daten aus Verfahren zu verwenden, in denen gar keine Straftat vorlag – wie beispielsweise aus dem Strafermittlungsverfahren, das die Staatsanwalt-

schaft Berlin wegen angeblicher Beleidigung gegen mich führte, um unter dem Vorwand von Strafermittlungen und unter der Andeutung schwerer Straftaten gegenüber der Bank mein Konto abzufragen. Die Kontendaten wurden trotzdem weitergegeben und anderweitig weiterverwendet. Eine Löschung der Daten trotz Löschanspruch verweigert.

Es geht hier zwar noch um Konto- und nicht um biometrische Daten, die Frage bleibt aber dieselbe: Würden diese Daten unter „aus einem Strafverfahren“ fallen und herangezogen werden dürfen?

Es geht aus dem Gesetzentwurf nicht hervor, ob bei gleicher Konstellation in vorgetäuschem Strafermittlungsverfahren erhobene Daten unter die Formulierung „aus einem Strafverfahren“ fallen und verwendet werden dürften.

Letztlich kann die Staatsanwaltschaft damit in gleicher Weise beliebig Ermittlungsverfahren fingieren, um biometrische Daten zu erfassen und verwenden. Mit Organisationen wie der Meldestelle RESpect!, HateAid, und „Hessen gegen Hetze“ hat bzw. hatte man zusammen mit §§ 130, 188 StGB eine Infrastruktur und einen Fundus, um aus politischen Gründen gegen jeden, der sich jemals kritisch geäußert hat, ein Ermittlungsverfahren zu fingieren und dann Ermittlungsbefugnisse anzuwenden (oder vorzutäuschen).

Zusammen mit den – meines Erachtens verfassungswidrigen – „Gummiparagrafen“ §§ 130 und 188 StGB kann man im Prinzip gegen jeden Regierungskritiker Strafermittlungsverfahren fingieren und dann per KI und Biometrie das Umfeld ausforschen – wie man es bisher mit Bankkonten gemacht hat. Dem politischen Missbrauch sind keine Grenzen mehr gesetzt.

Man kann dabei sogar – wie die Meldestelle RESpect! – so weit gehen, dass im Prinzip schon eine Strafanzeige mit bewusst unrichtigen oder unvollständigen, gezielt verfälschenden Daten mindestens ein Aktenvorgang ausgelöst wird, über den die Staatsanwaltschaft befinden muss, ob sie Ermittlungen darauf gründet. Weil der Begriff des „Strafverfahrens“ nicht definiert ist und theoretisch schon die Strafanzeige darunter fallen kann, steht es im Prinzip jedem offen, jedes beliebige biometrische Datum wie ein Foto oder Video durch anonyme Anzeige zum Gegenstand eines „Strafverfahrens“ zu machen – auch wenn gar keine Straftat vorliegt.

Es bedarf einer präziseren Abgrenzung, ab welcher Phase eines Verfahrens biometrische Daten aus demselben verwendet werden dürfen.

2.4 Begriff der „öffentlich zugänglichen Daten aus dem Internet“

2.4.1 „aus dem Internet“

Das ist als umgangssprachliche Formulierung scheinbar und laienhaft klar, aber tatsächlich sagt diese Formulierung gar nichts aus, denn „das Internet“ ist ein reines Transportmedium, in dem, auf dem, oder auch aus dem gar keine Daten kommen. Die Daten kommen von anderen, von Servern, von Diensten, die über das Internet erreichbar sind.

Dazu analog wäre, wenn Sie Rechtsfolgen nicht daran binden, um welche Art von Waren, Produkten, Drogen, Waffen es geht, etwa unerlaubten Drogen- oder Waffenbesitz, sondern daran, ob sie bei der Lieferung über die Autobahn oder die Paketpost transportiert wurden. Also würde man gesetzlich festlegen, dass der Besitz von Waffen dann legal ist, wenn sie bei der Lieferung über eine Autobahn transportiert wurden, weil Autobahnen öffentlich zugänglich sind.

Auch wenn derzeit keine Alternative zum Internet erkennbar oder absehbar ist, kann es trotzdem keine Rolle spielen, ob die Daten per Internet oder anderweitig transportiert werden. Das kann durchaus dann relevant werden, wenn große Datenmengen, KI-Sprachmodelle usw. per Datenträger und nicht per Internet angeliefert werden.

2.4.2 „öffentlich zugänglich“

Im Gesetzestext wird der Begriff der „öffentlich zugänglichen Daten“ verwendet, aber nicht näher erläutert. Erst in der Begründung auf Seite 14 heißt es

Unter öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Es sind auch solche Daten erfasst, die nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können. Nicht umfasst sind hingegen Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

Gilt das auch für illegal veröffentlichte Daten?

Was ist mit gestohlenen oder sonst widerrechtlich veröffentlichten Daten? Urheberrecht? Datenschutz?

Aktuelles Beispiel: Der Verwaltung von Berlin wurden – angeblich – vor einigen Tagen mehrere Terabyte Daten abgezogen und im Internet veröffentlicht, nachdem Berlin sich weigerte, das verlangte Lösegeld zu zahlen. *Dürften solche Daten verwendet werden?*

Nach der – rechtlich nicht maßgeblichen – Begründung wären sie von „jedermann“ zu verwenden.

Welches Recht, welchen Landes, wäre für die Frage der Rechtmäßigkeit anzuwenden?

Warum wird die Verwendung bei den Daten in Polizeisystemen an die Rechtmäßigkeit gebunden (§ 98e Abs. 1 StPO), nicht aber im Internet?

2.4.3 Jugendsperre

Die EU will gerade ein Social-Media-Verbot für Jugendliche durchsetzen.

Nach dem Wortlaut der Begründung wären Social-Media-Daten dann nicht mehr verwendbar, weil sie nicht mehr für „jedermann“, sondern nur für einen begrenzten Kreis (nämlich derer im Alter ab 14) zugänglich sind, **und der Zugang auf Zwang der EU einer Kontrolle unterzogen wird.**

Das ist also schon in sich nicht konsistent.

2.5 Begriff der „biometrischen Daten“

Der Begriff der Biometrie wird intensiv und zentral verwendet, aber nirgends definiert. Mir sind ad hoc keinerlei Definitionen im deutschen Recht außerhalb von DSGVO und BDSG bekannt. Artikel 4 Nr. 14 DSGVO:

„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

und § 46 Nr. 12 BDSG, nahezu gleichlautend:

„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

(Erläuterung: „physisch“ bezieht sich im allgemeinen Gebrauch auf äußerliche, unmittelbar wahrnehmbare, morphologische Eigenschaften wie Fingerabdruck, Gesichts- und Handgeometrie, Iris, den Körperbau, während „physiologisch“ eher funktionale, innere, funktions- und lebensbezogene Körpervorgänge bezeichnet, wie DNA, Venenmuster, Herzrhythmus.)

Da sich § 46 im drittem Teil des BDSG befindet, ist er nach § 500 StPO auf das

Strafrecht anwendbar.

Damit passt er aber nicht zur Gesetzesbegründung, wo es auf Seite 14 in 21/6806 heißt

Die Ermittlungsbeamten müssen eine tatsächliche **morphologische Übereinstimmung überprüfen** und prüfen, dass die ausgeworfenen **Lichtbilder** auch echt, also nicht KI-generiert sind.

Der Verfasser des Textes hat also – wohl irrtümlich – den Begriff der biometrischen Daten nur auf einen Teil der physischen, die morphologischen Eigenschaften bezogen, die durch einen Ermittlungsbeamten unmittelbar – am Bildschirm – überprüft werden können. Der Begriff geht aber technisch und auch nach der Definition in BDSG und DSGVO viel weiter. Was ist etwa mit

- dynamischen Eigenschaften wie dem Gang oder der Mimik?
- der DNA (etwa durch im Internet veröffentlichte DNA-Analysen)?
- Stimme, Aussprache, Dialekt (in einem Video oder Podcast)?
- sprachlichen Eigenschaften wie Worthäufigkeiten, Redewendung, Wortschatz, Formulierungen?
- Rhythmus von Tastaturanschlägen?
- Netzhaut, Venen, Herz?
- Fahrstil im Auto, etwa gemessen in einem Mietwagen oder einem PKW mit neuer EU-Fahrassistentenüberwachung?

Sind diese erfasst oder nicht?

Auch wenn Ihnen das abwegig erscheinen mag, weil es um im Internet frei zugängliche Daten geht: Ich habe als Blogger auch schon Fotos meiner Trommelfelle und von Magen- und Darmspiegelungen veröffentlicht. Dürften diese Bilder – etwa der darauf sichtbaren Blutgefäße – biometrisch herangezogen werden, oder nicht?

Das sind alles Eigenschaften, die zur Identifikation von Personen verwendet werden können und auch tatsächlich verwendet werden. Es gibt Verfahren, die anhand von Vergleichstexten recht gut feststellen können, wer einen Text verfasst hat. Alles das wird von § 46 Nr. 12 BDSG erfasst, passt aber nicht zur Begründung des Gesetzestextes.

Warum nicht? Weil DSGVO und BDSG eine *Negativabgrenzung* vornehmen, klarstellen, was man *nicht* darf, und deshalb *weit* gefasst sind. Die vorliegenden Gesetzentwürfe wollen aber eine *positive Gestattung* vornehmen, etwas erlauben.

Das geht schief, weil man – wenn man die Formulierung der Gesetzesbegründung heranzieht – weniger wollte als das BDSG definiert, und nicht gemerkt hat, dass es

nur eine Legaldefinition gibt, die als Negativabgrenzung sehr weit gefasst ist.

So ist der Begründung deutlich anzumerken, dass der Verfasser ausschließlich von Foto- und Videoaufnahmen ausging, andere biometrische Eigenschaften aber überhaupt nicht bedacht hat.

Dies ist besonders bezüglich der Erfassung von Ton und Text klärungsbedürftig.

Wie soll ein Ermittlungsbeamter eine morphologische Übereinstimmung überprüfen, wenn es um einen Podcast oder einen Text geht? Bei Ton und Video bezieht sich die Biometrie auf den Inhalt, also die Gezeigten. Bei Texten dagegen auf den Verfasser.

Was ist ein Echtzeit-Geschehen bei einem Text? Wenn ich die Gebäude des Bundestags als Text beschreibe, ist das dann ein Geschehen, was zum Zeitpunkt des Abgleichs noch stattfindet und deshalb nicht mehr verwendet werden darf (vgl. Abschnitt 2.6 unten)?

Das mag Ihnen nicht wichtig erscheinen, es kann aber äußerst wichtig werden – denken Sie an

- Erpresserbriefe (neulich Stadt Berlin)
- Bekennerschreiben auf Indymedia/LinksUnten zu Anschlägen auf die Infrastruktur oder Personen
- anonyme Postings in Social Media

Da können Textanalysen weit wichtiger werden, als der Verfasser sich das vorgestellt hat. Dann läuft die Vorschrift zur morphologischen Übereinstimmung leer.

Was ist, wenn die KI jemanden anhand

- der Stimme eines Sprechers
- der Bewegungen einer Person unter der Burka
- der Bewegungen eines Vermummten auf einer Demo

erkennt? Dürfen diese Daten dann verwendet werden? Wie soll der Ermittler sie „morphologisch“ prüfen?

Man merkt sehr deutlich, dass man den Gesetzestext einfach an der Causa Daniela Klette entlanggeschrieben hat und die nötige Sachkunde nicht hatte. Wenn man sich nur auf Bilder beziehen will, warum steht es dann nicht im Gesetzestext?

Dieser Gesetzentwurf ist nicht „gar“.

2.6 Begriff der „Echtzeitdaten“

Im beantragten § 98d Abs. 1 StPO heißt es

Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

Was sind „Echtzeitdaten“?

Beachten Sie, dass ich Informatiker bin und deshalb von Ausbildung und Berufs wegen weiß, was „Echtzeitsysteme“ sind, die in der Informatik eine wichtige Rolle spielen. Ich weiß schon, was das ist. Das Problem ist, dass es der Verfasser wohl nicht hinreichend wusste.

Der Begriff einer „Echtzeit“ bezieht sich – insbesondere in der Informatik – immer auf ein definiertes, vorgegebenes Zeitverhalten innerhalb eines definierten Zeitintervalls, innerhalb dessen reagiert werden muss. Es bedeutet nicht „gleichzeitig“, wie das hier gemeint ist, sondern „innerhalb einer spezifizierten und technisch sichergestellten Reaktionsfrist“. Subjektiv und umgangssprachlich „ohne wahrnehmbare Verzögerung“. Das ist hier nicht ersichtlich.

Technisch „echtzeitfähig“ war nur der rein analoge Rundfunk ohne Aufzeichnungen. Jede digitale Übertragung muss erst ganze Bilder einsammeln und sie komprimieren, dann in Datenpaketen übertragen und diese beim Empfänger wieder zusammensetzen. Das macht selbst im günstigsten Fall mehrere Sekunden aus, wie sich leicht beobachten lässt, wenn man „Live-Übertragungen“ gleichzeitig vor Ort und auf dem Fernseher beobachtet.

Probieren Sie es einfach aus:

- Lassen Sie während einer Bundestagsdebatte den Fernseher laufen und vergleichen Sie, wie lang es dauert, bis ein Bild ankommt.
- Besorgen Sie sich eine genau Uhr (DCF77, NTP, Internet, notfalls einfach das Handy) und schauen Sie die Fernsehnachrichten gleichzeitig auf einem DVB-* -Fernseher und per Streaming, und vergleichen sie bei allen drei Quellen, wann es da „20.00 Uhr“ ist.
- Schalten Sie das Radio an und hören Sie denselben Sender per Streaming.
- Kennen Sie den Effekt, dass etwa beim Fußball der Nachbar schon „Tor!“ schreit, wenn bei Ihnen der Stürmer erst auf der Mittellinie ist?

Selbst wenn man „Echtzeit“ als „so schnell, wie es eben geht“ definiert – was ist dann mit Streaming, wenn man die Pause-Taste drückt und später fortfährt? Oder mit der in vielen Ländern inzwischen gängigen Praxis, Livesendungen mit 2 Minuten Verzögerungen zu übertragen, um auf Störungen und Vorfälle rechtzeitig durch Ausblendung reagieren zu können?

Die Absicht dahinter (Seite 14 in 21/8606) ist gut gemeint, aber der Text schlecht gemacht. So sollen auch Sendungen erfasst werden, in denen das Publikum zu sehen ist. Viele Sendungen werden aber mittags aufgezeichnet und abends ausgestrahlt. Sind die Live? Sind die Echtzeit?

Was ist, wenn die Sendung nachts wiederholt wird? Oder in die Mediathek gestellt wird? Sind das dann auch „Echtzeitdaten“, oder sind sie das nicht mehr, obwohl derselbe Inhalt?

Was ist, wenn ich mich als Blogger vor den Bundestag stelle und etwas in die Kamera spreche – entweder aufgenommen oder live auf Youtube gestreamt – und im Hintergrund Abgeordnete vorbei laufen und im Bild zu sehen sind. *Sind das dann „Echtzeitdaten“?*

Der Begriff trägt nicht und ist ungeeignet. **Man hat das Problem gefühlt, aber nicht durchdacht.** Denn in der Erklärung (Seite 14) heißt es:

Nach Absatz 1 Satz 2 ist ein Abgleich mit solchen Daten unzulässig, die zum Zeitpunkt des Abgleichs ein tatsächliches Geschehen in Echtzeit widerspiegeln. Es soll damit ausgeschlossen werden, dass eine Echtzeitüberwachung bestimmter Bereiche stattfindet. Gemeint sind damit insbesondere Live-Streams, zum Beispiel von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam eines öffentlich zugänglichen Ortes. Erfasst sind auch Echtzeit-Lichtbild-Sequenzen, also beispielsweise die Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Die erklärte Absicht dahinter ist, dass das tatsächliche Geschehen zum Zeitpunkt des Abgleichs nicht mehr stattfindet¹.

Was ändert es an diesem Schutzzweck, wenn die Sendung nur aufgezeichnet und einen Tag später gestreamt, das Publikum aber trotzdem gezeigt wird? Wenn die Sendung in der Mediathek steht?

Was ist mit Dauerstreaming einer Webcam? Wann ist das nicht mehr „Echtzeit“?

Und wie passt es zum Zweck der Feststellung des Aufenthaltsorts eines Zeugen oder Beschuldigten, wenn der Abgleich erst dann erfolgen darf, wenn er nicht mehr dort ist?

Und wann gilt ein „tatsächliches Geschehen“ als beendet? Wenn ich mich vor den Bundestag setze und das live streame – wann gilt das dann als nicht mehr tatsächliches Geschehen? Wenn ich aufstehe und gehe?

Wo und wann endet ein „tatsächliches Geschehen“? Endet das tatsächliche Wohnen dann, wenn man da nicht mehr wohnt?

¹ Sie berücksichtigt schon nicht die Spitzfindigkeit der Juristen, die etwa schon ein Betrachten als „Vervielfältigung“ einstufen, weil die Daten in den Speicher kopiert werden müssen. Was werden die mit dem Begriff der „Echtzeit“ anfangen?

2.7 Reichweite des beantragten § 98d StPO

Die Formulierung des beantragten § 98d Abs. 1 StPO

Zur Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen dürfen biometrische Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen biometrischen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden, wenn ...

suggestiert bei oberflächlichem Lesen, dass es um die biometrischen Daten eines Beschuldigten oder Zeugen geht.

Liest man es aber genau, dann ist dies nur der *Zweck*. Um *wessen* biometrische Daten es geht, wer biometrisch identifiziert werden soll, steht – genau genommen – nicht da. Im Prinzip kann dies jede beliebige Person sein, sogar völlig unbeteiligte.

Es würde nach dieser Formulierung beispielsweise reichen, wenn in einem Strafverfahren auf einem Foto eine unbeteiligte Person zu sehen ist, die weder Beschuldigter noch Zeuge ist.

2.7.1 Beispiel: Ehefrau

Der Beschuldigte ist auf der Flucht. Mit seiner strafrechtlich unverdächtigen Ehefrau, die aber das Posten von Selfies auf TikTok nicht lassen kann.

Darf die Polizei nach diesem Gesetz dann also statt nach dem Beschuldigten selbst auch biometrisch nach dem Aufenthaltsort seiner Ehefrau suchen, weil man in der Akte ein Foto hat, das auch sie zeigt?

Dem Wortlaut des Textes nach: Ja. Der Begründung nach: Nein.

2.7.2 Beispiel: Klette/Garweg

Auf einem beschlagnahmten Handy findet man Fotos eines gesuchten Terroristen, und auf weiteren Fotos auf dem Gerät, die eindeutig in derselben Umgebung aufgenommen wurden, Fotos unbeteiligter Person, die zufällig vorbei lief, ohne von den Vorgängen zu wissen. Privatperson, Paketbote, Pizzafahrer, Schulkind auf dem Schulweg. Genau wie in der Causa Daniela Klette, auf deren Handy aktuelle Fotos vom ebenfalls gesuchten Burkhard Garweg gefunden wurden.

Das Foto dieser unbeteiligten Person – weder Beschuldigter, noch Zeuge – ist damit ein biometrisches Datum „aus dem Strafverfahren“.

Dürfte die Polizei also biometrisch nach dieser unbeteiligten Person suchen, um deren Wohn- und Arbeitsort zu ermitteln und daraus auf den abgebildeten Ort und daraus

auf den Aufenthaltsort des Terroristen zu schließen?

Ich halte die Formulierung nicht nur für ungenau, sondern für ungeeignet, weil sie bei wörtlicher Auslegung einen viel weiteren Handlungsspielraum lässt, als sie beim ersten, arglosen Lesen suggeriert.

2.7.3 Beispiel: Kinderpornographie

Ein klassischer und beim Bundeskriminalamt sehr häufig vorkommender Fall sind sichergestellte Fotos und Videos von Kinderpornographie, in denen Kinder gewaltsam missbraucht werden. Typischerweise sind die Kinder, aber nicht die Täter zu sehen. Das schreit geradezu als Anwendungsbeispiel, zumal das BKA hier über große Fotosammlungen verfügt.

Die Kinder sind nicht Beschuldigte, und wegen ihres Alters oft auch rechtlich und tatsächlich nicht Zeuge.

Dürfte nun die Polizei auch biometrische Daten der Kinder abgleichen, etwa um sie Jahre später, wenn sie älter sind und auf normalen Fotos und Filmen wie Klassenfotos oder Social Media Postings auftauchen, zu identifizieren, um den Tatort und die Täter zu finden?

Das geht für mich aus diesem Gesetzentwurf nicht klar hervor. Der Gesetzestext scheint es in seiner Ungenauigkeit herzugeben, die Begründung dagegen nicht.

2.7.4 Beispiel: Wohnzimmerschrankwand

Sowohl das BKA, als auch „Aktenzeichen XY ungelöst“ haben schon insbesondere bei Kinderpornographie, selten aber auch in anderen Fällen nicht nur nach Personen, sondern nach Möbeln, Räumlichkeiten, Einrichtungsbesonderheiten gesucht, etwa wenn auf Kinderpornofotos im Hintergrund das Wohnzimmer, die Schrankwand oder Ähnliches zu sehen ist, und die Vermutung naheliegt, dass jemand, der die Vorgänge nicht kennt, trotzdem schon mal in diesem Wohnzimmer war und die Einrichtung wiedererkennt.

Dürfte die Polizei per KI auch nach Fotos suchen, auf denen dieselbe Schrankwand, aber noch Personen oder andere hilfreiche Bildinhalte zu sehen sind? Auch Schrankwände sind personenbezogene Daten. Aber kaum biometrisch.

Oder herauszufinden, wer die gleiche Schrankwand besitzt oder sie verkauft hat, um zumindest das Land einzugrenzen oder beim Verkäufer zu fragen, an wen sie verkauft wurde?

2.8 Wieviel darf an die KI ausgelagert werden (Art. 33 Abs. 4 GG)?

KI schreibt längst Diplom- und Doktorarbeiten, Gutachten, Bücher.

Wie weit dürfen Staatsanwaltschaft und Polizei ihre Arbeit an die KI auslagern?

Darf man bei der KI ein Foto einwerfen und sagen „*Such mir den, finde Straftaten von ihm und schreib mir damit einen Haftbefehlsantrag und eine Anklageschrift!*“ ? Also letztlich die gesamte Arbeit von Polizei und Staatsanwaltschaft an die KI auslagern?

Wo ist die Grenze?

Ab wann wird die Ausübung hoheitlicher Befugnisse (Art. 33 Abs. 4 GG) vom Beamten auf die KI verlagert?

Bisher schon haben wir eine – meines Erachtens verfassungswidrige – ständige und vollautomatische Überwachung von Medien per KI durch Landesmedienanstalten.

Haben wir dann irgendwann eine automatisierte und eigenmächtig agierende KI-Polizei und KI-Staatsanwaltschaft, die das alles automatisch und ohne Menschen macht?

Ich wette, dass solche Produkte und Dienstleistungen in Bälde angeboten und – bei der Überlastung deutscher Staatsanwaltschaften – und genutzt werden.

2.9 Berufsgeheimnisse und Zeugnisverweigerungsrechte

2.9.1 Tracking von Verweigerungsberechtigten

Der Schutz von Aussage- und Zeugnisverweigerungsrechten kommt hier im Gesetztext nicht vor. Erst in der Begründung.

Das erscheint mir insbesondere deshalb kritisch, weil nach dem beantragten § 98d StPO nicht nur Beschuldigte, sondern auch Zeugen biometrisch gesucht werden können.

Hat jemand ein Zeugnisverweigerungsrecht, ob nun als Anwalt, Pfarrer, Arzt, oder auch als Vater, Mutter, Bruder usw. ändert das nichts daran, dass er als Zeuge benannt und geladen werden kann. Auch ein Pfarrer, Arzt, Vater hat als Zeuge zu erscheinen und seine Identität zu nennen. Er kann dann die Aussage verweigern, indem er sich auf das Zeugnisverweigerungsrecht beruft – was aber nichts daran ändert, dass er formal Zeuge ist (und u.a. als Zeuge entschädigt wird).

Nach dem Wortlaut des beantragten § 98d StPO könnte man aber über biometrische

Erkennung nachträglich verfolgen, wohin Anwalt, Pfarrer, Arzt, Bruder gegangen sind, um den flüchtigen Beschuldigten aufzusuchen.

Ähnliches gilt dann auch für Journalisten, die ebenfalls über ein – allerdings geringeres – Zeugnisverweigerungsrecht und Quellenschutz verfügen.

2.9.2 Ausweitung der Verstrickungsklausel

Bisher gelten für Berufsgeheimnisträger die Verstrickungsklauseln aus § 160a Abs. 4 und § 97 Abs. 2 Satz 2 StPO.

Danach sind Maßnahmen, Beschlagnahmen usw. gegen Berufsgeheimnisträger dann nicht anzuwenden, wenn sie selbst an der Straftat beteiligt sind oder Gegenstände aus einer Straftat haben.

Der beantragte § 98d StPO wendet die biometrische Verfolgung aber auch auf Zeugen an, und das Berufsgeheimnis schützt nur vor der Aussagepflicht, aber nicht vor der formalen Benennung und Ladung als Zeuge.

Berufsgeheimnisträger können damit also auch dann, wenn sie nicht unter die Verstrickungsklausel fallen und vor Aussagepflicht und Beschlagnahme geschützt sind, trotzdem über die biometrische Verfolgung ausgeforscht werden.

Es wird mir aus den Formulierungen nicht mit der nötigen Gewissheit klar, ob die biometrischen Maßnahmen von den Vorschriften über Berufsgeheimnisträger und Zeugnisverweigerungsrechte erfasst werden.

Erst in der Begründung auf Seite 14 von Drucksache 21/6806 findet sich

Der Schutz von Berufsgeheimnisträgern ist nach der allgemeinen Schutzvorschrift des § 160a StPO gewährleistet. Soweit das europäische Medienfreiheitsgesetz (European Media Freedom Act – EMFA) Gewährleistungen zum Schutz von Medienschaffenden enthält, sind diese von den Rechtsanwendern vorrangig zu beachten und bei der Anwendung des deutschen Rechts zu berücksichtigen

und auf Seite 22

Zu nennen ist auch der Schutz von Berufsgeheimnisträgern nach § 160a StPO. Demgemäß ändert sich auch das Niveau, mit dem Berufsgeheimnisträger geschützt sind, nicht. Soweit das europäische Medienfreiheitsgesetz (European Media Freedom Act – EMFA) Gewährleistungen zum Schutz von Medienschaffenden enthält, sind diese von den Rechtsanwendern vorrangig zu beachten und bei der Anwendung des deutschen Rechts zu berücksichtigen.

§ 160a Abs. 1 Satz 1 StPO lautet

Eine Ermittlungsmaßnahme, die sich gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2 oder Nummer 4 genannte Person, einen Rechtsanwalt oder einen Kammerrechtsbeistand richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig.

Die Gesetzesbegründung erscheint mir so nicht haltbar.

Denn bisher bezieht sich das Verweigerungsrecht von Berufsgeheimnisträgern eben auf deren Recht zur Verweigerung.

Wird also ein Anwalt, Arzt, Pfarrer, eine Verwandte als Zeuge befragt, oder ist Ziel einer Hausdurchsuchung oder Beschlagnahme, dass weiß und merkt er das, **weil ihm der Beschluss überreicht werden muss** und kann entsprechend erklären, dass er Aussage oder Beschlagnahme verweigert.

Beide, **Ärzte und Anwälte**, sind außerdem jeweils berufsrechtlich verpflichtet, **gut sichtbare Kanzlei- und Praxisschilder** an ihren Geschäftsräumen zu haben. Die Polizei könnte kaum eine Hausdurchsuchung oder Beschlagnahme vornehmen, ohne das Schild zu sehen.

Auch bei Maßnahmen einer Telefon- oder Internetüberwachung geht regelmäßig und notwendig die Identifikation des Anschlussinhabers voraus.

Wird jedoch nach einer Person biometrisch gefahndet, insbesondere bei der verfahrensübergreifenden Verwendung von Daten und der Fahndung nach Zeugen oder Unbeteiligten, ist noch gar nicht absehbar, ob die Betroffenen Berufsgeheimnisträger oder anderweitig verweigerungsberechtigt sind.

In Verbindung damit, dass Betroffene über die Maßnahmen auch nicht informiert werden, wenn sie nicht Beschuldigte sind (vgl. Abschnitt 3.1) erscheint mir diese Begründung recht leichtfertig und theoretisch.

Es scheint, als hätte man das Problem zwar erkannt, aber es übergangen und sich dabei nur so ein bisschen drumherum formuliert.

Gesetzesbegründungen werden zwar oft von Gerichten beachtet, falls denn irgendwer auf die seltene Idee kommt, sie zu lesen und darauf zu verweisen. Streng genommen sind sie aber rechtlich unbeachtlich und nur der blanke Gesetzestext zählt.

Und dann ist fraglich, woher die Polizei zum Zeitpunkt der Maßnahme wissen sollte, ob derjenige Berufsgeheimnisträger ist, und wie der sein Verweigerungsrecht beanspruchen können sollte, wenn er von der Maßnahme nie erfährt. **Es ist ja gerade als Zweck im beantragten § 98d Abs. 1 Nr. 2 StPO auch die Identitätsfeststellung als Zweck angegeben – wie soll man dann § 160a StPO anwenden, wenn man noch gar nicht weiß, wer die Person ist?**

Tief durchdacht ist das nicht, auch wenn § 160a vorsieht, dass „dennoch erlangte Erkenntnisse“ nicht verwendet werden dürfen.

Meine praktische Erfahrung ist, dass sich Polizei, Staatsanwaltschaft und Gerichte um solche Verbotsfeinheiten – jedenfalls in Berlin – nicht scheren und sie auch nicht kennen.

Mir jedenfalls hat die Eigenschaft als Berufsgeheimnisträger nach § 53 Abs. 1

Nr. 5 StPO gegen die Durchsuchung meines Kontos gar nichts genutzt. Das interessiert die Justiz überhaupt nicht. Das ist denen völlig egal, und sie kennen diese Vorschriften auch nicht.

2.9.3 Ausdehnung der StPO

Außerdem ist fraglich, ob § 160a StPO überhaupt in jedem Fall anwendbar ist. Denn bisher – und das wird ja in den Gesetzesanträgen auch als Problem angesehen – geht die StPO immer von einem in sich ge- und abgeschlossenen Verfahren aus.

Hier aber werden Ermittlungsmaßnahmen und die Datenanwendung *fallübergreifend* eingeführt, und die biometrischen Maßnahmen können sich dem Wortlaut nach auch auf unbeteiligte Dritte beziehen, was die Frage aufwirft, ob eine juristische Auslegung „vertretbar“ wäre, die die Maßnahme als nicht „gegen“ den Dritten gerichtet ansieht und deshalb § 160a StPO für nicht anwendbar erklären würde.

Es genügt deshalb nicht, § 160a StPO nur in der Begründung so ein kleines bisschen anzuerwähnen. Das beeindruckt das Gesetzgebungsverfahren, aber nicht Staatsanwälte und Richter.

Hier sind klare Formulierungen im Gesetzestext selbst erforderlich.

2.10 Misgendern

Sie als Gesetzgeber haben es verboten, Personen zu „misgendern“ (§ 14 SBGG).

Was ist nun, wenn sich jemand als Frau „identifiziert“, die KI die Person aber nach

- Aussehen
- Bewegungsablauf
- Körperbau und Skelett
- Stimme
- Sprechweise
- Verhaltensweise

als Mann erkennt?

Nach § 500 StPO i. V. m. § 58 BDSG sind die Daten dann als unrichtig auf Antrag der Betroffenen zu löschen oder deren Nutzung einzuschränken.

- Sind solche Daten „unrichtig“ i. S. d. § 58 Abs. 1 BDSG?

- Ist deren Verarbeitung „unzulässig“ i. S. d. Abs. 2?
- Oder ist deren Verarbeitung „einzuschränken“ i. S. d. Abs. 3?
- Ist der Abgleich eine rein informative Ermittlung, oder gilt sie als Beweiszweck i. S. d. Abs. 3 Nr. 2?

Das alles erschließt sich mir zumindest innerhalb der für die Stellungnahme zur Verfügung stehenden kurzen Zeit aus dem Gesetzestext nicht.

2.11 Datenschutz: Besondere Kategorien personenbezogener Daten

Der Datenschutz (hier 3. Teil BDSG, ansonsten DSGVO) stuft bestimmte Daten, wie die sexuelle Präferenz, die politische Meinung, die Religion als besondere Kategorien ein, deren Erhebung und Verarbeitung nicht oder nur unter besonderen Voraussetzungen möglich ist.

Wie aber ist das anzuwenden, wenn die im Internet öffentlich zugänglichen Daten, mit denen abgeglichen werden soll, etwa

- eine Kundgebung zugunsten der RAF,
- Teilnehmer des Christopher Street Days,
- rechte, linke, sonstwas-Demonstrationen
- islamistische Versammlungen
- sexualitätsbezogene Aufmachung

betreffen? Woran ist das zu erkennen?

Wird die Verarbeitung besonderer Kategorien dann dem Gutdünken der Polizei, der Lust und Laune der Datenschutzbeauftragten und der Tagesstimmung, der Zufallsrechtskunde, der mangelnden Sachkunde, der schmutzigen Phantasie und den Karriereinteressen der entscheidenden Richter überlassen? Wird sich schon irgendwie finden?

Wie stellt man sich das vor?

2.12 Indirekter Nutzen?

Die Ermittlungsbefugnis ist zweckgebunden, etwa für die Erforschung des Sachverhaltes, Feststellung der Identität oder des Aufenthaltsortes.

Ist dann der Abgleich auch mit Daten zulässig, die darüber keinen oder nur indirekten Aufschluss geben? Darf man also mit Fotos aus dem Internet abgleichen, die den Beschuldigten – und womöglich andere Personen – zeigen, die keinem dieser Zwecke zuträglich sind, etwa den Beschuldigten beim letzten Urlaub zeigen?

§ 98d Abs. 3 sagt hierzu, dass die Daten unverzüglich zu löschen seien, soweit sie keinen konkreten Ermittlungsansatz für das Verfahren oder ein anderes Strafverfahren aufweisen.

Das erscheint mir nicht umsetzbar, denn wie soll ein Ermittlungsbeamter „unverzüglich“ erkennen können, ob ein Bild, etwa die Schrankwand oder ein Gebäude im Hintergrund, einen „konkreten Ermittlungsansatz“, wenn sich dies erst später, mit weiteren Abgleichen herausfinden lässt?

Ein typisches Beispiel sind die gelegentlich öffentlich oder über die Sendung Aktenzeichen XY Ungelöst ausgestrahlten Fahndungen nach Kinderschändern, bei denen zum Schutz der Betroffenen keine Personen, aber auf Fotos sichtbare Einrichtungsgegenstände, Räume, Örtlichkeiten gezeigt werden, in der Hoffnung, dass jemand sie wiedererkennt.

Die Vorstellung, dass alles, was nicht unmittelbar einen konkreten und *erkennbaren* Ermittlungsansatz liefert, sofort zu löschen sei, ist praxisfern und nicht realistisch, sie entspricht nicht der typischen Vorgehensweise bei Suchmaschinen- oder KI-Recherche.

Man muss zunächst sammeln, einen Fundus aufbauen, auch von Daten, die einem zunächst nicht hilfreich erscheinen, um dann doch durch Kombination Erfolge zu erzielen.

In der Realität würde eine Suche nicht so ablaufen, dass man nur da weitersucht, wo sich ein Ermittlungsansatz ergibt, sondern mit zunehmender Suchtiefe und -komplexität eine immer größere Wolke aus zunächst scheinbar nutzlosen oder unzusammenhängenden Informationen ansammeln, bis sich daraus dann doch irgendwann ein Zusammenhang und Ermittlungsansatz ergibt, man die entscheidende Kleinigkeit, das nebensächliche Detail findet. Man sucht also nicht, *wo* sich ein Ermittlungsansatz ergibt, sondern *bis* sich ein Ermittlungsansatz ergibt. Das ist mit der Formulierung des Gesetzes unvereinbar, die erkennbar darauf ausgelegt ist, etwa das Bundesverfassungsgericht zu besänftigen.

Die Vorschrift ist nicht praktikabel. Wenn man aber praxisferne und kontraproduktive Gesetze macht, ist es so gut sie sicher, dass diese nicht eingehalten werden.

Ist die Vorschrift also naiv, oder von vornherein gar nicht beabsichtigt, dass sie eingehalten wird, und sie nur dazu da, um das Bundesverfassungsgericht zufriedenzustellen?

len?

2.13 „Spieglein, Spieglein an der Wand, wer ist die Schönste im ganzen Land?“

Den Gesetzentwürfen ist deutlich eine laienhafte, an die Nutzung von gewöhnlichen Suchmaschinen wie Google angelehnte Sichtweise anzumerken.

Es herrscht die Vorstellung, dass man „im Internet“ irgendwie ein Bild eines Gesuchten hochlädt, es dann kurz rumpelt, und man sich dann aus der Trefferliste das heraussucht, was einem eine Antwort auf die Frage liefert, und am besten gleich den Gesuchten im Strandcafé mit Name der Gaststätte, Straßennamen, Orts- und Zeitangabe. Feuchte Träume von Datenschützern.

So funktioniert das aber nur in seltenen, idealen Ausnahmefällen.

Man wird, ausgehend von dem Material, das man hat, mit einer zunehmenden Zahl von Indirektionsschritten eine immer größer werdende Wolke aus Informationen sammeln müssen, bis sich endlich ein verwertbarer Informationspfad findet. Frei erfundenes Beispiel:

- Die KI findet biometrisch ein Foto vom Verdächtigen, wie er in unbekannter Gaststätte feiert.
- Die KI findet dazu ein Foto einer anderen Person, die zu einem anderen Zeitpunkt ohne Bezug zum Verdächtigen in derselben Gaststätte saß.
- Die KI findet von dieser unbeteiligten Person ein anderes Foto, aus dem hervorgeht, dass sie am Ort X arbeitet. Die Gaststätte könnte sich also in der Nähe der Arbeitsstelle befinden.
- Die KI listet alle ihr bekannten Gaststätten in einer 10km-Umgebung um X.
- Auf Google Street View lässt sich eine Gaststätte finden, die zu den Fotos passen könnte.
- Der Verdächtige könnte sich also in der Umgebung der Gaststätte aufhalten.

Die Vorstellung, dass man biometrisch mit dem Passfoto des Gesuchten wie in der Google Bildersuche anfragt, und sich aus den Antworten eine heraussucht, die einen zum Gesuchten führt, ist nur in seltenen Ausnahmefällen möglich und damit nicht realistisch.

Insbesondere findet sich darin dieselbe Mentalität wieder, mit der man in Deutschland hohe Standards der Sozial- und Arbeitssicherheit durchsetzt, und dann immer mehr Produktion in Billiglohnländer auslagert, um diese eigenen hohen Standards wieder

zu umgehen.

Man tut hier so, als würde man klimaneutrale, wunderbar saubere Elektroautos fördern, aber lagert die Sauerei, das Material für die Akkus zu schürfen, einfach ins ferne Ausland aus.

Auf dieselbe Weise wird hier ein hohes Datenschutzniveau vorgegaukelt, und gleichzeitig dessen Verletzung ins Ausland ausgelagert. Man täuscht hier vor, dass man nur eng am Fall und nur die notwendigen Daten speichere, hehre Datenschutzambitionen verfolge, nutzt aber gleichzeitig ausländische (insbesondere US-amerikanische) Datenbanken und KI-Systeme, die sich um unseren Datenschutz nicht scheren.

Wir haben eine hohe Divergenz zwischen dem, was die Entwürfe an Datenhygiene suggerieren und versprechen, und dem, wie es dann läuft. In der Praxis ist das nicht umsetzbar. In der Praxis wird das zu riesigen Vorratsdatenbanken führen, auch weil KI-Systeme möglichst viele Bilder brauchen, um nach einer Person zu suchen. Man tut so, als würde man hier nur das Allernötigste speichern und verwenden, übergeht dabei aber völlig, dass man nicht einfach mal so ohne Datenbestände „im Internet“ biometrisch nach einer Person suchen kann. Wie stellt man sich das vor? Einfach mal „das Internet“ fragen?

Man stellt das hin, als gebe es da ein „frei zugängliches Internet“, für das man rechtlich nicht verantwortlich sei, am besten noch im Ausland außerhalb unserer Regierungsverantwortung, und dem man einfach so Fragen stellt wie die Königin dem Spiegel im Märchen von Schneewittchen: *„Spieglein, Spieglein an der Wand, wer ist die Schönste im ganzen Land?“*

Haben Sie sich jemals gefragt, welche Mengen an personenbezogenen Daten aller Frauen im Land der Spiegel erhoben, gespeichert und verarbeitet haben muss, um darauf eine Antwort geben zu können? Um

- daraus anhand biometrisch-morphologischer Daten die Schönste zu finden,
- deren Aufenthaltsort zu nennen,
- auch noch deren Mitbewohner
- und damit besondere Kategorien personenbezogener Daten (Sexualleben und sexuelle Orientierung § 46 Nr. 14e BSDG)

anzugeben? Offensichtlich nicht, sonst würde man so ein Gesetz nicht schreiben. Jedenfalls nicht so.

Stattdessen streiten Sie mit dem Spiegel um „diskriminierende“ (oder wie die Grünen – siehe 9.3 – um „rassistische“) Algorithmen beim Schönheitsvergleich.

Die böse Königin hält sich datenschutzrechtlich für unangreifbar (Verfolgung eigener Interessen, Auslagerung an den Spiegel). Da irrt sie. Tatsächlich nämlich betreiben Königin und Spiegel eine Auftragsdatenverarbeitung, und damit ist die Königin für die

Datenhaltung des Spiegels mit verantwortlich.

Nicht anders verhält es sich, wenn die Polizei die KI fragt, wo und bei wem sich die Beschuldigte aufhält, und um aktuelle biometrisch-morphologische Daten zum Abgleich ersucht. KI-Antwort: „*Hinter den sieben Bergen, bei den sieben Zwergen – und sie ist tausendmal schöner als Ihr.*“

Was hier normiert wird, ist letztlich eine Auftragsdatenverarbeitung, für die, zunächst anlasslos, das gesamte Internet, alle Social Media, alle Webseiten, alle Bücher, einfach alles, was an Informationen greifbar ist, erfasst und in Datenbanken abgelegt, analysiert, vernetzt wird.

Und dann tun Sie hier so, als hätten sie damit gar nichts zu tun, weil Sie ja nur mal fragen, und dann alle Antworten „unverzüglich löschen“, die nicht sofort zum Ziel führen und damit notwendig sind.

Die Realität ist, dass man hier nicht nur enorme, sondern effektiv *die totale* Datenerfassung betreibt und zur Fahndung nutzt, und das hinter Formulierungen aus Auslagerungen versteckt.

Die Regierung betrügt damit sich selbst, die Öffentlichkeit und das Bundesverfassungsgericht. Die merken das nämlich nicht.

2.14 Datenflut der USA

In den USA ist das Datenschutzniveau bekanntlich deutlich niedriger als in der EU, und eine Reihe von Firmen bauen in den USA gerade für monströse Beträge KI-Rechenzentren, zu deren Funktionen es ohne Zweifel gehören wird, sämtliche Publikationen und öffentlich verfügbaren Daten zu erfassen und erkennen.

Es wird

- Autorenprofile
- Pseudonymauflösungen
- Anonymauflösungen (insbesondere Antifa, Linksextremismus usw.)
- Komplette Personendossiers zu nahe zudem westlich, durch Reisen oder in der IT jemals in Erscheinung getretener Person

geben. Man wird keine Bewerbungsschreiben mehr brauchen, weil die KI bereits alles über einen weiß.

Schon heute verlangen die USA bei der Einreise die Darlegung von Verwandtschaftsverhältnisse, aller jemals verwendeten Social Media Accounts, Zugangspassworte und so weiter und so fort. Es steht außer Frage, dass sich die USA nicht nur bei der Ein-

reise, sondern generell bei jeder Person und zu jedem Zeitpunkt dafür interessieren. Man wird jede Person immer und ständig identifizieren und ausnahmslos alle – öffentlichen und nichtöffentlichen – Äußerungen und Darstellungen von Personen erkennen wollen.

Schon jetzt haben wir Funktionen bei Youtube u.ä., die gesprochenes Wort erkennen und automatisch Untertiteln oder in andere Sprachen übersetzen können. Es ist eine Frage der Zeit, bis auch auf jedem Video eingeblendet wird oder werden kann, wer im Video gerade zu sehen ist.

Dies gibt es bereits im Bereich des kommerziellen Streamings von Kinofilmen usw. auf Amazon Prime. Bei fast allen Filmen kann man jederzeit die Pausetaste drücken und sich anzeigen lassen, welche Personen als Rolle gerade im Bild zu sehen sind, und durch welche Schauspieler sie dargestellt werden. Das wird es auch über kurz oder lang auf Youtube, Twitter, TikTok, Instagram usw. geben.

Werden dann auch diese Daten erfasst und abgeglichen?

2.15 Beweislast?

Wer trägt die Beweislast dafür, dass Internet-Daten, mit denen abgeglichen wurde, echt und unverändert oder eben nicht echt, nicht unverändert sind?

Muss die Polizei die Echtheit beweisen, oder ist es Aufgabe des Beschuldigten, deren Unechtheit nachzuweisen?

Ab wann gelten Daten als unecht? Ist ein Video noch morphologisch echt, wenn die KI die Sprache übersetzt? Und dazu die Stimme nachahmt? Die Mundbewegungen anpasst?

Wo ist die Grenze?

Und wieso sollen ausgerechnet Richter, die als Juristen darin überhaupt nicht ausgebildet sind, darüber entscheiden können?

2.16 Haftung?

Wer haftet, wenn die KI sich irrt und später, wenn man den Falschen festgenommen oder verurteilt hat, im typischen KI-Ton säuselt „*Oh, Du hast recht. Ich habe mir geirrt. Danke, dass Du mich korrigierst!*“?

Die Polizei? Der KI-Betreiber? Social Media?

Anders gefragt: Wie sieht eigentlich die Vertragslage zwischen Polizei und KI-Betreiber

oder Social Media aus?

Was ist die Rechtsgrundlage von „frei verfügbar“ und nach dem Recht welchen Landes richtet sich das?

2.17 Evaluierung?

Von der Absicht, eine Evaluierung durchzuführen, ob das Verfahren funktioniert, wie es soll, habe ich nichts entdeckt.

3 Beeinträchtigte Grundrechte

3.1 Rechtswegsgarantie (Art. 19 Abs. 4 GG)

Die beantragten Vorschriften sehen keine Pflicht und kein Verfahren vor, den Betroffenen zu informieren.

Beschuldigte eines Verfahrens sind normalerweise entweder anwaltlich vertreten oder verfügen über eigene Rechtskunde, und wissen, dass sie Akteneinsichtsanspruch haben und nehmen diesen auch pflichtgemäß wahr. Man kann davor ausgehen, dass ein Beschuldigter bei angemessener Verteidigung aus den Akten über die biometrische Fahndung erfährt und sich gegebenenfalls zur Wehr setzt.

Auch das ist allerdings nicht sicher, denn viele Strafverteidiger sind der Auffassung, dass man sich möglichst still und unauffällig verhalten müsse, solange keine Anklage erhoben wurde. Auch werden die Kosten eines Anwaltes vorher nicht ersetzt, weshalb viele Beschuldigte vor Erhebung der Anklage keinen Anwalt haben und keine Akteneinsicht nehmen. Wird das Verfahren eingestellt, erfahren sie nie von einer biometrischen Fahndung.

Bei Zeugen oder Unbeteiligten ist dies aber – insbesondere wegen der hier eingeführten fallübergreifenden Datenverarbeitung – nicht der Fall. Ein Zeuge hat keinen Anspruch auf Akteneinsicht, und in der Regel auch keinen Grund, Akteneinsicht zu begehren, weil er durch das Verfahren an sich nicht beschwert und für seine Aufwände entschädigt wird.

Wie sieht der Rechtsweg aus, wenn man Gegenstand einer biometrischen Suche, aber nicht Beschuldigter ist?

3.2 Meinungsfreiheit (Art. 5 Abs. 1 GG)

Im Verfassungsrecht der USA gibt es den Begriff des „chilling effect“, wenn eine Maßnahme ein Grundrecht nicht unmittelbar und direkt bedroht, sie aber einen Abschreckungs- und Einschüchterungseffekt hat, etwa dessen Wahrnehmung mit einem Risiko oder empfindlichen Nachteil einhergeht. Solche Maßnahmen gelten als verfassungswidrig.

Auch in der Rechtsprechung des Bundesverfassungsgerichts war der Gedankengang,

dass ein Grundrecht nicht unmittelbar, aber durch Abschreckung beeinträchtigt wird, schon zu finden.

Wenn, wie hier, nicht nur – wie laut Begründung gewollt – das Aussehen, morphologische Eigenschaften, sondern – nach dem Wortlaut – auch Bewegungen, die Stimme, die Art zu sprechen oder zu schreiben erfasst werden (können), und damit jede praktikable Art und Weise, seine Meinung zu äußern, und es damit auch unmöglich wird, seine Meinung öffentlich ohne Namensnennung, unter Pseudonym, anonym kundzugeben, weil bei jeder Äußerung nicht nur zu fürchten ist, dass deren Inhalt sofort erfasst und per KI massenhaft verarbeitet, und damit auch mündliche Äußerungen „verstanden“ werden, sondern auch die Identität des Sprechers erkannt wird, und das so abgespeichert wird, dass jederzeit die Zuordnung von Person zu allen ihren Äußerungen, oder von Äußerungen eines gewissen Inhaltes zu allen Personen, die sich jemals derartig geäußert haben, möglich wird, hat das eine massiv abschreckende Wirkung.

Aus demselben Grund halte ich auch den Medienstaatsvertrag der Bundesländer bezüglich der Überwachung von Medien für verfassungswidrig.

3.3 Pressefreiheit (Art. 5 Abs. 1 GG)

Im Gegensatz zum Recht vieler anderer Länder umfasst die Pressefreiheit in Deutschland nicht das Recht zur Äußerung (das fällt hier unter die Meinungsfreiheit), sondern das Recht auf Recherche und Information.

Wenn aber bereits die bloße Anwesenheit an einem Ort und ein Tracking der Bewegung über die biometrische Erkennung (oder Mobilfunk) schon erfasst wird, und zwar auch dann, wenn man nur Zeuge oder Unbeteiligter ist, der allein deshalb überwacht wird, weil daraus auf den Aufenthaltsort eines Beschuldigten geschlossen werden kann, liegt darin eine Verengung und Einschränkung der Pressefreiheit.

3.4 Versammlungsfreiheit (Art. 8 GG)

Dasselbe gilt für die Demonstrations- und Versammlungsfreiheit. Wenn bereits die reine Anwesenheit an einem Ort massenhaft erfasst und ausgewertet werden kann und wird, hat dies einen abschreckenden Effekt auf die Wahrnehmung dieses Grundrechts.

4 Verhältnismäßigkeit

4.1 „auch im Einzelfall erhebliche Bedeutung“

Der beantragte § 98d Abs. 1 Nr. 1 StPO sieht vor

... bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat und, ...

Dies suggeriert, dass es um schwere Straftaten gehen müsse, was bei genauem Lesen aber nicht der Fall ist. Denn die Formulierung „im Einzelfall erhebliche Bedeutung“ (oder „schwer wiegt“) wird oft auch schon im Falle der Beleidigung (§ 185 StGB), insbesondere aber der Politikerbeleidigung (§ 188 StGB) angewandt, um

- die Bedingung des § 100a Abs. 1 Nr. 2 StPO zu erfüllen, auch wenn keine Katalogstraftat vorliegt,
- um die Bedingung des § 188 StGB „sein öffentliches Wirken erheblich zu erschweren“ zu erfüllen.

Mitunter vertreten Staatsanwälte und Richter auch die Auffassung, dass die „im Einzelfall erhebliche Bedeutung“ im Strafverfahren stets erfüllt sei, weil man sonst ja gar nicht erst ermitteln würde.

Es ist eine bis zur Beliebigkeit dehnbare Gummiformulierung, die effektiv die biometrische Fahndung für jede beliebige Straftat öffnet.

Faktisch heißt das nur, dass der Staatsanwalt einen Zettel mit der Verfügung in die Akte legen muss, dass die im Einzelfall erhebliche Bedeutung bejahe. Oder das auf dem Aktenvorblatt einfach ankreuzt. Eine semantische Bedeutung wohnt dem nicht inne.

4.2 Fehlende Voraussetzung schuldhaften Verhaltens

Der beantragte neue § 98d StPO enthält die Formulierung

Zur Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder **eines Zeugen** ...

ist zwar an nachfolgende Bedingungen geknüpft, wie etwa

... bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat ...

was aber schon zeigt, dass es sich dabei **nicht um dieselbe Person handeln muss**, denn ein Zeuge steht ja nicht im Verdacht, eine Straftat begangen zu haben. Somit sind also – folglich auch beim Beschuldigten – der biometrisch gesuchte Beschuldigte (oder Zeuge) nicht mit dem identisch, der im Verdacht einer solchen Straftat steht.

Letztlich müssen die beiden noch nicht einmal im selben Strafverfahren beschuldigt und verdächtigt sein. Insbesondere Zeugen können hier ohne jegliches schuldhaftes, verwerfliches, rechtswidriges Verhalten in den Sog biometrischer Fahndung geraten. Dazu kommt, dass ein Zeuge, im Gegensatz zu einem Beschuldigten, nicht gehalten ist, sich erreichbar zu halten.

Ich halte das für unverhältnismäßig. Eine solche Maßnahme kann meines Erachtens nicht ohne die Anordnung der zwangsweisen Vorführung eines Zeugen vertretbar sein.

5 Missbrauch

5.1 Missbrauch von innen

5.1.1 Politischer Missbrauch

Ich habe es gerade selbst miterleben müssen: Staatsanwaltschaft und Landeskriminalamt Berlin haben zum Schein ein Strafermittlungsverfahren gegen mich geführt, weil ich nach § 188 StGB eine Politikerin beleidigt hätte, obwohl keine Straftat vorlag und von der Staatsanwaltschaft auch nicht ernstlich dargelegt werden konnte.

Mehr noch: Die Akten zeigen, dass die Staatsanwaltschaft und das LKA sich für die angebliche Straftat nicht interessiert haben und nicht einmal auf die Idee gekommen sind, die fragliche Äußerung überhaupt zu sichten oder zu sichern.

Das Verfahren diene nur als Vorwand, um für den Verfassungsschutz – wie öffentlich von Nancy Faeser und dem Bundesverfassungsschutz angekündigt – ein Konto auszuspionieren und dessen Kündigung zu bewirken.

Rechtsschutz dagegen hat sich in Berlin, Wiesbaden und Karlsruhe als unmöglich erwiesen. Die Rechtswegsgarantie ist ein Witz.

Es besteht kein Zweifel, dass dieselbe Staatsanwaltschaft und dasselbe Landeskriminalamt mit derselben kriminellen Energie auch Strafermittlungen als Vorwand für biometrische Abgleiche vortäuschen würden.

Ich sehe in diesem Gesetzentwurf keinerlei Maßnahmen, um dies zu verhindern, und keinerlei Rechtsschutz. Man vertraut laut Begründung naiv, blind und leichtfertig darauf, dass die Datenschutzbeauftragten das Ding schon irgendwie schaukeln werden.

Die Erfahrung zeigt aber, dass sie das nicht tun. Nicht können, politisch nicht dürfen, und jedenfalls in Hessen auch nicht wollen.

5.1.2 Unterwanderung durch organisierte Kriminalität

Es gibt Gerüchte und Behauptungen, etwa die Berliner Polizei sie längst korrupt und von Clans systematisch unterwandert, die nicht nur passiv Informationen über Polizeiaktionen abgreifen, sondern sich auch aktiv polizeilicher Befugnisse bemächtigen, um Gegner anzugreifen oder Verfahren gegen sie zu „bestellen“.

Sie müssen sich von der Vorstellung lösen, dass die Polizei und die Staatsanwaltschaft immer „Die Guten“ wären. Das sind sie schon lange nicht mehr. In Berlin sind die Strafverfolger mitunter krimineller als die Verfolgten. Und es hat seinen Grund, warum die Polizeien anderer Bundesländer – sowohl im hier relevanten Fall der Festnahme von Daniela Klette, also auch im Fall der Juwelen aus dem Dresdner Grünen Gewölbe – die Berliner Polizei nicht mehr vorab einweihen, damit die die Informationen nicht an Clans oder RAF durchstechen?

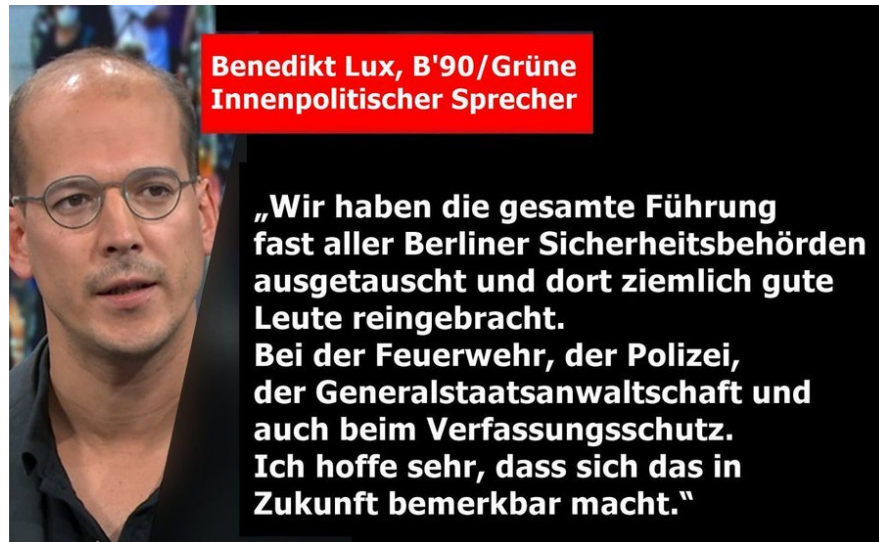
Was ist eigentlich, wenn die Clans – in Berlin haben wir inzwischen praktisch täglich Schießereien – oder der nächste islamistische oder russische Attentäter Polizeibefugnisse durch Innentäter oder vorgetäuschte Anzeigen verwenden, um eine gegnerische Person, etwa Zeugen oder Politiker, Verräter, Geheimdienstmitarbeiter, Aussteiger, V-Leute zu finden und umzulegen?

5.1.3 Unterwanderung durch Linksextremismus

Dieselbe Frage stellt sich bei Linksextremismus und Antifa, die bekanntlich ebenfalls auf Menschenjagd geht. Beispiel: „Lina E.“.

Just als ich diesen Text hier schreibe hat gerade DIE LINKE die Wahl zum Abgeordnetenhaus in Berlin gewonnen und wird voraussichtlich die regierende Bürgermeisterin stellen.

Ist die LINKE in der Regierung, sind Polizei, Antisemitismus und linker Terror nicht mehr voneinander zu trennen. Dann sitzt die Neo-RAF praktisch in der Landesregierung als Vorgesetzte der Polizei und besetzt die Posten. Der LKA-Beamte, der mein Bankkonto ausspioniert hat, ist zumindest namensgleich, vermutlich identisch, mit einem Ex-Politiker der Piratenpartei. Da werden Personenverbindungen unter dem Vorwand von strafrechtlichen Ermittlungen ausspioniert.



(Graphik Internet-Meme)

Ich kann bestätigen, dass sich das bemerkbar macht.

Grünen-Organisationen wie Meldestelle REspect! und HateAid haben mit der Berliner Justiz eine feste grüne Infrastruktur zur Verfolgung von Kritikern gebildet, die – wie in meinem Fall – polizeilich Befugnisse nicht nur für politische Zwecke missbraucht, sondern sogar in strafbarer Weise überschreitet.

5.1.4 Akteneinsicht

Während meiner Tätigkeit für die Vorratsdatenspeicherung 2009 hatte ich einige Gespräche mit Staatsanwälten, weil ein Unternehmen, das urheberrechtlich geschützte Produkte vertrieb, Raubkopien systematisch ermöglichte, manche sagten, provozierte, um dann Strafanzeige zu erstatten.

Strafanzeigen verliefen stets ergebnislos, wurden immer eingestellt. Die Staatsanwaltschaft musste aber stets zunächst per IP-Adresse und Vorratsdatenspeicherung den Beschuldigten ermitteln, woraufhin dann das Unternehmen Akteneinsicht nahm, Namen und Anschrift fand, und dann abmahnte, was das eigentliche Geschäft war.

Wie stellen Sie sicher, dass dieselbe Masche nicht auch mit Biometrie abläuft? Dass also Unternehmen Anzeige gegen jemanden erstatten, der fotografiert wurde, ihn über die Staatsanwaltschaft biometrisch identifizieren lassen, um dann als Geschädigte Akteneinsicht zu nehmen?

5.2 Fälschung und Täuschung von außen

Je bekannter die Ermittlungsmethoden werden, desto eher werden sie auch zur Fälschung, Diffamierung, falschen Anschuldigung missbraucht.

Gibt es nicht gerade Diskussionen um „Deep Fakes“? Laufen die Social Media nicht über vor Fake-Videos von allem und jedem?

Geradezu herzlich naiv ist da die Gesetzesbegründung (Seite 14 in 21/6806):

Die Ermittlungsbeamten müssen [...] prüfen, dass die ausgeworfenen Lichtbilder auch echt, also nicht KI-generiert sind. Erst bei einem positiven Ergebnis kann der Treffer Ausgangspunkt für weitere Ermittlungsmaßnahmen sein.

Wie prüft denn ein Ermittlungsbeamter, ob „*Lichtbilder auch echt*“ sind?

Wenn Sie wissen, wie das geht, haben Sie den Beruf verfehlt. Dann sollten Sie keine Gesetzes-, sondern Patentanträge schreiben.

Ich war selbst Ziel von Verleumdungen und Angriffen aus dem linksextremen Milieu. Nach Recherchen zu Gender Studies wurde ich von der Berliner Antifa u.a. massiv am Arbeits- und Wohnort diffamiert, und in Briefkasteneinwürfen und im Internet (Indymedia/Linksunten) als „Holocaustrelativierer“ beschimpft, obwohl ich nie etwas derartiges geäußert habe oder äußern würde.

Ich war 2023 als Sachverständiger für den Bundestag zur Vorratsdatenspeicherung tätig, meine Stellungnahme hat aber wohl nicht allen gefallen, denn ich wurde – mit ausdrücklichem Bezug darauf – von der grünennahen „Kontext Wochenzeitung“ unter Wiederholung dessen erneut als „Holocaustrelativierer“ hingestellt. Begründen oder belegen konnte sie das – selbstverständlich – nicht.

Aus demselben grünen Stuttgart („Meldestelle RESpect!“) erfolgte eine Strafanzeige gegen mich, die den Tatbestand einer falschen Verdächtigung erfüllt, weil man aus einem rund 10-seitigen Text einen einzelnen Satz ausgeschnitten und den per Screenshot so hingestellt hat, als hätte ich diesen einzelnen Satz ohne jeden Kontext geäußert. Die kriminelle Energie zur Fälschung lag offensichtlich vor, es fehlte nur an den technischen Möglichkeiten. Das ist heute anders.

Wäre derselbe Vorgang 3 Jahre später passiert, hätte man mit Sicherheit Fake-Bilder und Fake-Videos verbreitet, oder mein Blog gehackt, um nach außen und gegenüber der Staatsanwaltschaft den Vorwurf „zu belegen“.

Bereits jetzt ist „das Internet“ voll von KI-Fakes zur Diffamierung von Personen und zur Falschinformation, Verleumdung.

Wir stehen unmittelbar davor, mit Falschinformationen überschwemmt zu werden. Dann werden die „Belege“ für die bisher unhaltbaren, frei erfundenen Falschbehauptungen beigelegt und in Umlauf gebracht.

Es ist nicht nur längst Stand der Technik, dass die KI das Aussehen von Personen austauschen oder ganze Vorgänge fälschen kann, und es kein Problem mehr ist, jede beliebige Person als Pornodarsteller, Nazi, Kinderschänder, Idioten, was auch immer darzustellen. **Wir sind inzwischen an dem Punkt, an dem die KI selbst den Plan bilden und den Entschluss fassen kann, jemanden per gefälschtem Video zu kompromittieren und das Video auch noch selbst in Umlauf zu bringen. Es bedarf keines menschlichen Täters mehr.**

Ich erinnere an die Abgeordneten Jörg Tauss und Sebastian Edathy.

Es ist längst im Bereich des Möglichen, jemandem ohne dessen Wissen Kinderpornos auf den Rechner zu spielen, die er nicht bemerkt, die aber im Wege der Beschlagnahme und forensischen Untersuchung gefunden würden, und gleichzeitig gefälschte Kinderschänderpornos in Umlauf zu setzen, auf denen der Betroffene biometrisch identifizierbar als Täter dargestellt wird, so dass die Polizei diese zwangsläufig finden, denjenigen identifizieren und dann auf dessen beschlagnahmten Rechner die „Beweise“ finden würde. Die Verurteilung ist damit praktisch sicher.

Und dann kommen Sie daher und erklären in grenzenloser Naivität, der Ermittlungsbeamte müsse „prüfen, dass die ausgeworfenen Lichtbilder auch echt, also nicht KI-generiert sind.“

Wer schreibt sowas?

5.3 Naive Sicht auf Aufsichtsbehörden

Zur Missbrauchskontrolle findet man auf Seite 20 in 21/8606:

Die Begründungspflicht und die Protokollierung bei der Nutzung des Analysetools sichert die aufsichtliche Kontrollmöglichkeit durch den zuständigen Datenschutzbeauftragten und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes (vergleiche auch Gesetzesbegründung zu § 25a HSOG, Drucksache des **Hessischen** Landtags 20/11235, Seite 17).

Das ist ein Witz.

Ich bin seit Jahren damit befasst, gegen eine rechtswidrige Kontenabfrage eines Spendenkontos meines Blogs (als Publizist bin ich Berufsgeheimnisträger und die Daten als solche, aus denen die politische Meinung hervorgeht, eine besonders geschützte Kategorie von personenbezogenen Daten) und die Datenweitergabe durch die Staatsanwaltschaft und das Landeskriminalamt Berlin im Jahr 2023.

- Die Berliner Beauftragte für Datenschutz und Informationsfreiheit ist zwar vordergründig meiner Meinung, es passiert effektiv aber gar nichts.

Die Behörde ist überlastet und kann, will (und darf?) sich gegenüber Polizei und Staatsanwaltschaft nicht durchsetzen.

- Der **Hessische** Beauftragte für Datenschutz und Informationsfreiheit (zuständig für die Deutsche Bank mit Sitz in Frankfurt/Main) ist sogar kontraproduktiv.

Er verteidigt eine völlig rechtswidrige Datenweitergabe nach einem Phantasieverfahren ohne Rechtsgrundlage und meint, die Deutsche Bank sei vom Datenschutz entbunden und müsse und dürfe gar nichts prüfen, sondern der Polizei blind vertrauen und alle angefragten Daten bereitwillig und ohne jede Prüfung oder Rechtsgrundlage einfach so herausgeben.

- Das zuständige Verwaltungsgericht Wiesbaden ist so überlastet, dass auf Jahre hinaus nicht einmal an einen Verfahrensbeginn zu denken ist und die Angelegenheit bis dahin längst verjährt ist.

Es ist nicht nur blanker Hohn, wenn die Regierung meint, „effektiver Rechtsschutz“ würde durch die zuständigen Datenschutzbeauftragten gewährleistet, *und sich dabei auch noch ausgerechnet auf Hessen bezieht, wo der Datenschutz weit unter Null ist und politisch massiv sabotiert wird.*

Die Regierung als Antragsteller dieses Gesetzentwurfs zeigt damit sehr deutlich, dass sie entweder unredlich ist und bewusst täuscht – oder nicht weiß, wovon sie redet. Womöglich sogar beides.

Das Land Hessen hat sich in Datenschutzfragen völlig disqualifiziert.

Von der „Gewährleistung effektiven Rechtsschutzes“, zu der auf die „Gesetzesbegründung zu § 25a HSOG, Drucksache des Hessischen Landtags **20/11235**, Seite 17“ verwiesen wird, ist dort nichts zu finden, was diesen Anspruch trägt. Da steht nur

Satz 6 regelt die Befugnis des behördlichen Datenschutzbeauftragten, stichprobenartige Kontrollen durchzuführen. Im Zusammenspiel mit den in Abs. 5 geregelten (Satz 2) bzw. bekräftigten (Satz 3) Kontrollbefugnissen der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit gewährleistet diese Bestimmung eine effektive, zwischen behördlichem und unabhängigem Datenschutzbeauftragten aufgeteilte Kontrolle. Dass im Rahmen dieses abgestuften Kontrollkonzepts ein stichprobenartiges Vorgehen ausreichend ist, hat das Bundesverfassungsgericht ausdrücklich festgestellt (BVerfG, a. a. O., Rn. 109).

Das ist leeres Blabla. Die Praxis ist, dass der Hessische Beauftragte für den Datenschutz, Alexander Roßnagel, oder jedenfalls seine Behörde, sich mit Händen und Füßen dagegen wehrt, die Polizei zu überwachen und der Meinung ist, dass die Polizei tun und lassen kann, was sie will, und andere – wie die Deutsche Bank – zu gehorchen und blind darauf zu vertrauen haben, dass die Polizei schon weiß, was sie tut, und sich von selbst an das Gesetz hält, sie ist ja schließlich die Polizei.

Das Datenschutzniveau in Hessen ist weit unter Null.

Es ist kein Wunder, dass ausgerechnet Hessen bei solchen Gesetzen und der IP-Adressspeicherung federführend und Protagonist ist.

Und es entsteht in beiden Fällen der Eindruck, dass das Land Hessen auch über die

Gesetzesanträge auf Bundesebene bestimmt und die Bundesregierung deren Wünsche nur durchreicht und als ihre Anträge ausgibt. In der IP-Adressspeicherung ist dies überdeutlich, und auch hier entsteht dieser Eindruck.

Teil II

Antrag der Bundesregierung zur Polizeiarbeit (21/6132)

6 Unklarheiten, Fehler, Inkonsistenzen

6.1 Bezugnahme auf die StPO-Kritik

Zur Vermeidung von Wiederholungen und weil die vorliegende Stellungnahme unter hohem Zeitdruck erstellt wurde, verweise ich auf die oben in Kapitel 2 zur StPO-Änderung gemachten Ausführungen, die wegen der großen Ähnlichkeit der Texte auch hier zutreffen.

So finden sich auch hier die Unklarheiten zum Begriff der „Biometrie“, die oben ausführlich betrachtet wurden, oder der Begriff der „Echtzeitdaten“ (§ 9a BKAG).

6.2 Datenaustausch mit Drittstaaten

§ 9a Abs. 6 BKAG soll den Abgleich von Daten mit Stellen in einem Drittstaat ermöglichen.

Die mir zur Verfügung stehende Zeit erlaubte mir nicht, ausreichend zu prüfen, ob dies mit EU-Datenschutz-Recht vereinbar und ob hier EU-Recht oder nur Bundesrecht anwendbar ist, weil die Zuständigkeit der EU zwar den Datenschutz, nicht aber das Strafrecht umfasst.

Die Frage ist relevant, weil die USA zu den im Bereich der politischen Kriminalität und Terrorvorsorge wichtigsten Staaten gehört, die Formulierungen aber so weit gefasst sind, dass sie auch einfachste Straftaten erfassen.

6.3 Diskrepanz zwischen § 9a und § 9b BKAG

In § 9a Abs. 1 Nr. 1 BKAG soll es heißen

... dass eine Straftat von auch im Einzelfall erheblicher Bedeutung, **insbesondere** eine in § 100a Absatz 2 der Strafprozessordnung bezeichnete Straftat begangen worden ist ...

Hier wird also der Kreis **weiter gezogen** als im Katalog § 100a Abs. 2 StPO, nämlich der ganze Katalog **zuzüglich** der willkürlich auszulegenden Gummiklausel, die alles umfasst.

In § 9b Abs. 1 Nr. 1 dagegen heißt es

... dass eine Straftat im Sinne des § 100a Absatz 2 der Strafprozessordnung begangen worden ist, die Tat auch im Einzelfall schwer wiegt **und** ...

Hier wird also der Kreis durch die Und-Verknüpfung **enger gezogen** als der Katalog des § 100a Abs. 2 StPO.

Ist das Absicht und gewollt, oder redaktionelle Nachlässigkeit?

6.4 Selbstlernende Systeme

§ 22 BKAG erlaubt die Nutzung von personenbezogenen Daten

... zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme ...

Ebenso § 46 BPolG.

Mir wird daraus nicht klar, wie das dann mit dem Anspruch auf Löschung, Berichtigung oder Einschränkung der Verarbeitung aus § 58 BDSG zu vereinen ist. Man kann im Allgemeinen aus „selbstlernenden Systeme“ einzelne, spezifische Informationen nicht ohne weiteres isoliert entfernen oder ändern.

6.5 Auslagerung in die USA?

Sind § 63b Abs. 6 BKAG und gleichgelagert § 58a Abs. 6 BPolG zur Auslagerung des Abgleichs in Drittstaaten, insbesondere weil er nach Abs. 5 über die Auslagerung in EU-Staaten folgt, sich also **ausdrücklich auf Nicht-EU-Staaten bezieht**, weil für EU-Staaten Abs. 5 subsidiär wäre, so zu verstehen, dass wesentliche Teil der KI-Arbeit und Abgleiche des Bundeskriminalamts in die USA, an deren Rechenzentren, CIA und FBI ausgelagert werden?

In der Begründung auf Seite 19 heißt es

Im Rahmen der Ausübung der Befugnis ist die Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, erlaubt.

Faktisch also mindestens die USA.

6.6 Richtervorbehalt

§ 9a Abs. 8 BKAG sieht für die Auslagerung des Abgleichs in Staaten außerhalb der EU einen Richtervorbehalt vor.

Wieviele Richter gibt es in Deutschland, die technisch hinreichend verstehen, was hier passieren soll?

Es besteht meines Wissens für einen nach Geschäftsverteilung zuständigen Richter keine Möglichkeit, sich für unzuständig oder befangen zu erklären, wenn er die Sache technisch nicht versteht.

6.7 „diskriminierende Algorithmen“

§§ 9b Abs. 5, 22 Abs. 3, 63c Abs. 5 BKAG, sowie §§ 46 Abs. 3, 58b Abs. 5, sowie Seiten 29 und 31 sprechen von „diskriminierenden Algorithmen“.

Das ist technischer Unfug.

Es gibt keine „diskriminierenden Algorithmen“. Das ist politisches Modegefasel, und wer davon redet, hat nicht verstanden, was ein Algorithmus ist. Man verwendet das Wort so gerne, weil es sich so technisch und gelehrt anhört, aber insbesondere in Politik und Journalismus ist es nur Nachgequatsche.

Hierzu ausführlicher unten in Abschnitt [9.3](#).

6.8 § 15b verunglückt

In 21/6132, auf Seite 17 unten, vorletzter Absatz, fehlt im § 15b Abs. 2 Satz 1 Asylgesetz ein Satzteil.

6.9 Falscher Begriff der Gewährleistung

§ 9b Abs. 6 Satz 1 BKAG besagt

Das Bundeskriminalamt **gewährleistet** im Rahmen der Regelung der Zugriffsberechtigungen nach § 15, dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu **gewährleisten**, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

Hier wird der falsche Begriff verwendet.

Die Gewährleistung (Mängelhaftung) ist bzw. war die gesetzliche Verpflichtung eines Schuldners, dafür einzustehen, dass eine erbrachte Leistung oder verkaufte Ware zum Zeitpunkt des Übergangs frei von Sach- und Rechtsmängeln ist oder für eine bestimmte Gewährleistungsfrist funktioniert.

Die Gewährleistung heißt nicht, dass jemand etwas sicherzustellen oder durchzusetzen hat, sondern dass er für die Kosten haftet, wenn es die zugesicherten Eigenschaften nicht hat.

Wer die Gewährleistung für eine Waschmaschine trägt, hat nicht dafür zu sorgen, dass sie nicht kaputtgehen kann, sondern er hat die Reparaturkosten zu tragen, wenn sie kaputt geht. Er kann die Qualität auch bleiben lassen und einfach das Kostenrisiko tragen, denn es ist nicht festgelegt, *wie* eine Gewährleistung zu erfüllen ist.

Diesen Begriff hier zu verwenden würde nicht bedeuten, dass das Bundeskriminalamt die Schulung der Mitarbeiter und der Schutz gegen unbefugte Kenntnisnahme durchzusetzen oder sicherzustellen hat. Es würde bedeuten, dass das Bundeskriminalamt schuldrechtlich für den Schaden haftet, falls es schief geht.

Das kann nicht gewollt sein und wäre nicht zulässig.

Oder wollen Sie hier tatsächlich eine Mängelhaftung für das Bundeskriminalamt einführen?

7 Verhältnismäßigkeit

7.1 Bezugnahme auf die StPO-Kritik

Zur Vermeidung von Wiederholungen und weil die vorliegende Stellungnahme unter hohem Zeitdruck erstellt wurde, verweise ich auf die oben in Abschnitt 4 zur StPO-Änderung gemachten Ausführungen, die wegen der großen Ähnlichkeit auch hier zutreffen, etwa wenn auch hier Gummiformulierungen wie „*Straftat von auch im Einzelfall erheblicher Bedeutung*“ zu finden sind, die in der Praxis einfach alles bedeuten können und eine Abgrenzung nur suggerieren, aber nicht enthalten.

Teil III

Antrag der Bundesregierung zur Terrorismusabwehr (21/6131)

8 Unklarheiten, Fehler, Inkonsistenzen

8.1 Bezugnahme auf die StPO- und Polizei-Kritik

Zur Vermeidung von Wiederholungen und weil die vorliegende Stellungnahme unter hohem Zeitdruck erstellt wurde, verweise ich auf die oben in Kapitel 2 zur StPO-Änderung und in Kapitel 6 zu Polizeirechten gemachten Ausführungen, die wegen der großen Ähnlichkeit der Texte auch hier zutreffen.

Auch hier findet sich wieder die Formulierung „Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 der Strafprozessordnung bezeichnete Straftat“, an der ich oben bereits Kritik geäußert habe.

Ebenso Formulierungen wie „in Echtzeit“ oder „diskriminierende Algorithmen“.

Ich verzichte darauf, die bereits geäußerte Kritik zu wiederholen.

8.2 Sicherung von Verkehrsdaten

8.2.1 Thematische Zuordnung

Ich bin erstaunt, den Antrag für § 10b BKAG *hier* zu finden. Ich hätte den thematisch dem Gesetzentwurf zur IP-Adressspeicherung zugeordnet.

Es erweckt den Eindruck, als wollte man im Windschatten der Biometrie/Daniela Klette unauffällig schon so ein bisschen Vorratsdatenspeicherung einführen.

Kann es sein, dass hier verschiedene Akteure konkurrierend aneinander vorbei gesetzen?

8.2.2 Zeitpunkt

Ich kann der Formulierung für § 10b BKAG ad hoc nicht entnehmen, ob dies auch rückwirkend gelten soll, ob also auch Verkehrsdaten aus der Zeit **vor der Anordnung** erfasst werden, die – aus welchen Gründen auch immer – beim Anbieter von Telekommunikationsdienstleistungen noch vorliegen.

8.2.3 Was sind „Verkehrsdaten“?

Während der Begriff der Verkehrsdaten bei Telefonie recht eindeutig ist, ist er bei Internetdiensten – und § 10b BKAG soll alle Telekommunikationsdienste erfassen – durchaus nicht eindeutig.

Eine Legaldefinition findet sich in § 9 TDDDG, eine andere in § 3 Nr. 70 TKG, die schon nicht deckungsgleich sind.

Erst in dem einzufügenden § 52 Abs. 1 BKAG kommt der Verweis auf § 3 Nr. 70 TKG, während dort kurioserweise die Definition im alten § 52 Abs. 1, die noch auf §§ 9 und 12 TDDDG verwies, entfernt wurde.

Es scheint, als kämen die einzelnen Änderungen von verschiedenen Autoren und wären nicht angeglichen worden.

Gerade mit Hinblick auf Provider-NAT usw. wirft das erhebliche Fragen auf, welche Daten genau davon erfasst werden und aufgezeichnet werden müssen und dürfen.

Ich halte das deshalb für verfrüht, denn diese Diskussion ist zur IP-Adressspeicherung erst noch zu führen.

Teil IV

Gegenanträge

9 Antrag der Grünen (21/6913)

9.1 Kommentar statt Antrag

Der Antrag der Grünen (21/6913) ist bereits der Sache nach kein Antrag, sondern ein Kommentar, der nur pro Forma in einen Pseudoantrag gehüllt wurde. Ein greifbarer Antrag ist über „Der Bundestag möge beschließen, sich unserer Meinung anzuschließen“ nicht enthalten.

9.2 Leeres Blabla

Der Antrag ist leeres Blabla und Werfen mit Worthülsen und Buzzwords.

In der Informatik nennen wir das „Bullshit Bingo“. Man kann sich mit Pappkarten der aktuell angesagten Modewörter in einer Tabelle hinsetzen, sie beim Zuhören abhaken, und wer zuerst alle in einer Spalte oder Reihe abgehakt hat, ruft laut „Bingo!“ und hat gewonnen.

9.3 „Algorithmen“

Als Informatiker komme ich aber – wieder einmal – nicht umhin, und ebenso häufigen wie unsachgemäßen Gebrauch des Begriffs der Algorithmen zu rügen:

Zudem besteht die Gefahr diskriminierender Algorithmen, die unter anderem zu rassistischen Ergebnissen führen können. Neue Befugnisse für die Behörden müssen diese Risiken von vornherein adressieren und Sicherungsmaßnahmen, wie die Verpflichtung zur Erstellung von Schutzkonzepten vor diskriminierenden Algorithmen, umfassende Protokollierungspflichten, Maßnahmen zur Qualitätssicherung oder Transparenz und Nachvollziehbarkeit der Entscheidungsfindung vorsehen.

Bingo!

Auch wenn man noch so gerne „rassistisch“, „diskriminierend“ und „Algorithmen“ sagt, wird es durch Umrühren nur umso schlimmer.

Es gibt keine „diskriminierenden Algorithmen“, und wer das behauptet, hat den Begriff nicht verstanden.

Ein Algorithmus ist eine für einen bestimmten (auch hypothetischen, fiktiven, theoretischen) Maschinentyp ausgelegte, geordnete und ausführbare Zusammenfügung von Anweisungen, meist, aber nicht notwendigerweise in zeitlicher Abfolge, einer *gegebenen* Funktion. Vereinfacht ausgedrückt: Ein Algorithmus bringt einem bestimmten Maschinentyp bei, auszurechnen, was er ausrechnen soll, aber er bestimmt nicht darüber, was das Ergebnis ist.

So gibt es, als einfaches Beispiel, ganz verschiedene Sortieralgorithmen, die sich unterschiedlich verhalten und verschiedene Eigenschaften haben, aber das Ergebnis, die Elemente der Eingabe zu sortieren, ist immer dasselbe, weil der Algorithmus nicht darüber zu bestimmen hat, was die Sortierreihenfolge ist.

Genauso gibt es Algorithmen für Arithmetik, die addieren, multiplizieren und so weiter, aber keiner davon bestimmt darüber, was sie Summe oder das Produkt von Zahlen ist. Es gibt keine „diskriminierungsfreien Multiplikationsalgorithmen, die andere, politisch korrektere Ergebnisse liefern“. Das Produkt zweier Zahlen ist eine bestimmte Zahl, und der Multiplikationsalgorithmus hat sie zu bestimmen.

Algorithmen können korrekt (oder eben nicht korrekt) sein, sie können effizient, schnell oder langsam, teuer oder sparsam sein.

Aber „rassistisch“ oder „diskriminierend“ können sie nicht sein.

Wer so etwas von sich gibt, der zeigt sehr deutlich, dass er keine Ahnung hat, wovon er redet, und nur mit inhaltslosen Phrasen und Modebegriffen um sich wirft.

Wie man im Zeitalter der Digitalisierung und der Omnipräsenz von Computern als Fraktion eines Parlamentes eines ehemals führenden Industriestaates so wenig Ahnung von IT aufbringen kann, ist mir schleierhaft.

9.4 Keine Stellungnahme

Der Antrag ist Gefasel aus den einschlägig bekannten ideologischen Dauerphrasen und Versatzstücken. Eine darüber hinaus gehende Stellungnahme ist mangels Substanz nicht angezeigt.

10 Antrag der Linken (21/6917)

10.1 Positionierung statt Antrag

Im Gegensatz zum Antrag der Grünen enthält der Antrag der Linken (21/6917) einen greifbaren, konkreten Antrag (nämlich die Ablehnung des Gesetzesantrags), und er ist trotz seiner Kürze deutlich besser ausgearbeitet als der der Grünen.

Mit den Gesetzentwürfen sollen Befugnisse geschaffen werden, das gesamte Internet nach biometrischen Daten – nicht nur Gesichter, sondern auch andere biometrische Merkmale wie Stimme oder Bewegungsabläufe – zu durchforsten und sie in einer Datenbank zu sammeln. Diese sollen dann zur Identifizierung und Aufenthaltsermittlung von Personen genutzt werden, denen die Sicherheitsbehörden eine Gefahr für die öffentliche Sicherheit unterstellen oder die tatverdächtig sind. Durch die Befugnis, einen solchen Massendatenabgleich auch zur „Aufklärung eines Sachverhalts“ zu nutzen, soweit dies „erforderlich“ ist, öffnet dies die Tür für die Nutzung biometrischer Massenabgleiche als neues Standardinstrument der Polizei. Die dahinter stehende Logik, umfassend personenbezogene Daten aller Bürgerinnen und Bürger für noch unbekannte Zwecke in der Zukunft zu speichern, zu sammeln, zu verknüpfen und automatisiert auszuwerten, widerspricht dem Recht aller Einzelnen auf freie Entfaltung ihrer Persönlichkeit ohne die Angst, permanent Objekt staatlicher Ausforschung zu werden.

Das ist zutreffend erkannt und präzise formuliert. Das ist genau das, worauf die Anträge der Regierung hinauslaufen.

Eine Begründung der Vorwürfe fehlt dagegen. Hätte ich nicht gerade selbst die Anträge der Regierung durchgearbeitet und wäre zu ähnlichen Ergebnissen gekommen, fiel es mir schwer, die Vorwürfe nachzuvollziehen.

Die Möglichkeit der Identifizierung jeder Person sowie die Erstellung von Profilen über diese, würde bedeuten, dass es bei der Ausübung von Grund- und Freiheitsrechten keinerlei Anonymität mehr gäbe. Das Vertrauen, sich ohne das Gefühl permanenter Überwachung im öffentlichen – auch im digitalen öffentlichen – Raum anonym bewegen zu können, ist jedoch Voraussetzung für die Wahrnehmung zentraler Grund- und Freiheitsrechte wie das Recht auf freie Entfaltung der Persönlichkeit, der Versammlungs-, Vereinigungs- und Meinungsfreiheit und ist damit zentrale Voraussetzung einer freiheitlichen und offenen Demokratie. Nicht die lückenlose Erfassung der Bevölkerung, sondern geschützte Räume persönlicher Freiheit sind deren Fundament.

Auch das halte ich für zutreffend und richtig erkannt.

Der Antrag enthält die Sichtweise der Linken, aber er begründet sie nicht. Er entbehrt jeglicher Begründung, und ich kann die Aussagen nur deshalb nachvollziehen, weil ich die Anträge der Regierung selbst durchgearbeitet habe und zu ähnlichen Ergeb-

nissen gekommen bin. Für den unvorbereiteten Leser sind diese Vorwürfe mangels Begründung nicht verständlich und nicht nachvollziehbar.

Inhaltlich ist das eine Positionierung, eine Mitteilung des eigenen Standpunktes, aber kein substantieller Antrag.

Der Text wirkt in seiner geschliffenen und kompakten Darstellung abgeschrieben oder von außen zugeliefert und nicht authentisch. Er passt stilistisch und intellektuell nicht zu den sonstigen Äußerungen der LINKEN. Die KI dürfte inzwischen in der Lage sein, über die Vermessung der Sprache den Autor des Textes einzukreisen.

10.2 Politische Absichten

10.2.1 RAF und linker Terror

An diesem Text fällt mir mehr noch als das, was darin steht, das auf, was *nicht* darin steht. Nämlich die Nähe zwischen der Partei DIE LINKEN und der RAF und heutigem Linksextremismus.

Gerade weil Daniela Klette als Präzedenzfall über Biometrie identifiziert wurde und es heute praktisch nicht mehr möglich ist, der Biometrie zu entkommen – selbst Geheimdienste haben heute das Problem, dass die Tarnidentitäten ihrer Argenten auffliegen, weil sie in ihrer echten Identität etwa als Kind oder Schüler auf Fotos im Internet und in Social Media zu finden sind – drängt sich doch sehr der Verdacht auf, dass die Fraktion hier die Interessen ehemaliger und aktueller Linksterroristen vertritt. Linker Terrorismus wird ja auch als ein Grund für die Anträge genannt.

Eine Distanzierung der Linken von linker Gewalt gibt es nicht nur nicht, sondern es sind linke Positionen zu vernehmen, die noch mehr Gewalt fordern oder eine Eskalation der Gewalt ankündigen, insbesondere wenn der Wähler nicht so wählt, wie Linke es wünschen, oder sich nicht jeder dem Marxismus anschließt.

Gerade weil die vorliegenden Regierungsanträge offensichtlich am Fall Daniela Klette entlangformuliert sind, und es reichlich Solidaritätsbekundungen aus dem politischen Umfeld der Linken zugunsten der drei gesuchten RAF-Mitglieder gab, und die jahrelange Existenz Klettes wohl kaum ohne Unterstützung möglich war, liegt über dem Antrag der Odor unlauterer Absichten, nämlich der Interessenvertretung Krimineller und politischer Straftäter. Die Verstrickung mit den Anschlägen auf die Infrastruktur und die Bekennerschreibe auf Indymedia/Linksunten sind beredt, und die Linke muss sich auch die Frage gefallen lassen, inwieweit sie die Absicht verfolgt, Polizeiarbeit zu behindern, um ihr politisch nahstehende Kriminalität als politisches Mittel zu ermöglichen und die Täter zu schützen.

Letztlich wirkt der Text auf mich, als beantrage die RAF selbst, für sie unangenehme Ermittlungsbefugnisse und -methoden abzulehnen.

Ich erinnere daran, dass die damalige RAF von der SED unterstützt und gesteuert wurde, und die heutige LINKE mit der SED identisch oder zumindest deren Nachfolgerin, und aktuell ist ein Wiedererstarken oder der Aufbau einer neuen Generation der RAF zu beobachten. Auch die RAF hat damals mit Anschlägen gegen Sachen angefangen, und die Forderungen nach Gewalt gegen Personen stehen bereits wieder im Raum.

Ein wesentlicher Unterschied zum RAF-Terror der 70er Jahre ist, dass heute der öffentliche Raum vor Kameras und Social Media strotzt, und deshalb die Taktiken der RAF heute so nicht mehr funktionieren würden – obwohl der Fall Daniela Klette und Burkhard Garweg zeigen, dass sie durchaus bis vor Kurzem noch funktioniert haben. Der Fall Klettes zeigt aber, dass neue Techniken wie die KI-Identifizierung genau dieses Existenzmuster der RAF brechen.

Die LINKE muss sich fragen lassen, ob sie hier Absichten und Interessen verfolgt, die mit der Verpflichtung von Parteien zu unserer Grundordnung unvereinbar sind.

10.2.2 Migration und Islamischer Staat

Dieselbe Frage wiederholt sich in Bezug auf Migration, Terror, Hamas, Islamischer Staat, Antisemitismus.

Die Regierungsanträge nennen den Islamischen Staat als einen der zentralen Gründe für die Erforderlichkeit der Rechtsänderungen.

Auch hier ist die LINKE zunehmend mit den Gefährdern verwoben. Es gibt Behauptungen und Gerüchte, wonach die LINKE sogar zunehmend von Islamisten unterwandert werde und sich von der Marxisten- in eine Islamistenpartei verwandle.

Auch hier stellt sich die Frage, ob die Ablehnung auf gerade der kriminellen Interessenlage beruht, die die Regierung zu bekämpfen versucht.

10.3 Wertung

Der Antrag der Linken

- ist sehr gut, prägnant und präzise formuliert,
- erkennt und benennt die Gefahren und Problem gut und zutreffend,
- enthält eine konkrete und greifbare Antragstellung.

Er ist aber in der Substanz viel zu kurz. Eine Begründung fehlt und der Antrag ist nur für den verständlich, der zuvor die Regierungsanträge durchgearbeitet und bereits selbst zu diesem Ergebnis gekommen ist.

Die Antragstellung ist zwar konkret und greifbar (Ablehnung), ist aber nur komplementär zum Antrag der Regierung. Inhaltlich läuft es nur darauf hinaus, den Regierungsantrag abzulehnen und keinen eigenen Antrag zu stellen.

Der Antrag ist damit redundant, in gewisser Weise überflüssig. Es ist lediglich eine formal als Antrag formulierte Mitteilung des Standpunktes der Fraktion.

Der Antrag ist zwar beachtlich, aber er enthält nichts, was über die Abhandlung der Regierungsanträge hinaus inhaltlich noch zu bearbeiten wäre.

Eine explizite Stellungnahme zu diesem Antrag ist daher nicht angezeigt.

Teil V

Ergebnis

11 Regierungsanträge

11.1 Gesamtergebnis

Die Anträge sind – zumindest bis auf Weiteres – abzulehnen.

Sie sind handwerklich mangelhaft, unfertig, fehlerhaft, inkonsistent, praxisuntauglich und qualitativ nicht gesetzeswürdig. Zu vieles ist unlogisch, selbstwidersprüchlich oder überlässt es der Rechtsprechung, sich Reime darauf zu machen, was man selbst nicht verstanden hat.

Die Anträge sind ungar, unausgegoren, und erkennbar ohne die nötige Sach-, Rechts- und Realitätskunde erstellt. Sie wirken, wie von einem Theoretiker im Elfenbeinturm erstellt, der die Realität „da draußen“ nicht kennt.

Auffällig – und Beleg für die mangelnde Sachkunde – ist dabei die Divergenz und Diskrepanz zwischen der Vorstellung des Verfassers, oder besser gesagt, der Verfasser, die sich in der Gesetzesbegründung findet, und dem wörtlichen Regelungsgehalt im Gesetzestext.

So geht aus der Begründung hervor, dass sich der Verfasser da irgendetwas mit Bildern und Morphologie vorstellte, mangels Sorgfalt aber vergessen hat, den Begriff der Biometrie zu definieren, einzugrenzen oder wenigstens nach bestehenden Definition zu forschen, womit das dann in die Definition des BDSG fällt, die als *Negativabgrenzung* zum Zwecke des Verbots den Begriff weit fasst, und hier damit Tür und Tor für alles Mögliche geöffnet werden. DIE LINKE hat das durchaus auch erkannt.

Diese Gesetzesentwürfe würden ihrem Wortlaut nach Methoden erlauben, die der Autor anhand seiner Begründung erkennbar nicht beabsichtigt, und an die er auch nicht gedacht, die er sich nicht vorgestellt hat.

Das ist Schlamperei.

Und wenn erkennbar ist, dass schon der tatsächlich vorgelegte Antrag vom subjektiven Antragswillen abweicht, ist der Antrag abzulehnen und eigentlich sogar unzulässig, weil es am Willen fehlt.

Es drängt sich geradezu auf, dass man hier jemandem, der nicht in der Materie steckte, den Auftrag gegeben hatte, irgendwas zu schreiben, damit die EU und das Bundesverfassungsgericht in ihren Forderungen nach Gesetzesgrundlagen zufriedengestellt werden, und dabei einfach am Fall Daniela Klette – dem bisher herausragenden Präze-

denzfall – entlangzuschreiben. Diese Entwürfe bedürfen mindestens einer erheblichen Überarbeitung und der Klärung, was es eigentlich werden und erlauben soll.

Rechtsschutz, Gefahrenabwehr, Umgang mit Missbrauch, Grundrechtgewährung kommen darin nicht nur nicht vor – Äußerungen wie die aus der Begründung, dass sich der Ermittlungsbeamte überzeugen müsse, dass die Bilder auch echt und kein KI-Fake seien, sind von einer geradezu treuherzigen Naivität und einer Internet=Neuland-Mentalität, die wir eigentlich schon vor zwei Bundestagswahlen abgewählt hatten. Trockener betrachtet ist das laienhafte Hilflosigkeit vor der Problemstellung.

Herzlich naiv und weltfremd ist auch die Vorstellung, dass die Landesdatenschutzbeauftragten schon für effektiven Rechtsschutz und deren Durchsetzung stünden. Durch gelegentliche Stichproben. Das können sie weder rechtlich, von ihrer Stellung her, noch tatsächlich von ihrer Arbeitsbelastung her, und sie wollen es auch nicht, wenn sie – wie in Hessen – politisch besetzt sind, sich um Datenschutzrecht nicht scheren und politische Ziele verfolgen.

Doch ausgerechnet Hessen mit einem Datenschutzniveau unter Null ist nicht nur der politische Treiber hinter diesen Rechtsänderungen wie auch der IP-Vorrats-/Adressspeicherung. Mir drängt sich der Eindruck auf, dass Hessen auch mehr als nur politisch hinter diesem Antrag steht. Bundesländer sind aber im Bundestag nicht antragsberechtigt.

11.2 Ergänzende Begründungen

11.2.1 Position zur Biometrie

Ich bin nicht grundsätzlich gegen biometrische Fahndungsmethoden.

Im Gegenteil: Es wäre kaum zu vermitteln, warum man gesuchte Schwerverbrecher nicht auf diese Weise sucht oder deren Identität ermittelt. Der Fall Daniela Klette – 150 Meter von meiner Wohnung entfernt¹ – ist nicht nur ein Grund für meinen persönlichen Wunsch nach besserer Fahndung, sondern zeigte in der öffentlichen Diskussion und auch im Gespräch mit Nachbarn, dass in der breiten Bevölkerung Unverständnis darüber herrscht, solche Suchmethoden *nicht* anzuwenden. Die Frage wurde breit geäußert, warum die Polizei da nicht selbst drauf gekommen sei. Ich halte es für vertretbar zu sagen, dass eine zumindest gefühlte demokratische Legitimation besteht.

Man kann es aber nicht so schlampig normieren.

Außerdem habe ich es gerade selbst erlebt, dass die Staatsanwaltschaft und das Landeskriminalamt Berlin als Vorwand ein Strafermittlungsverfahren gegen mich führten, obwohl gar keine Straftat vorlag, und sich auch für die angebliche „Straftat“ gar nicht

¹Ich lege aber großen Wert auf die Feststellung, dass dies in Kreuzberg passierte und ich in Mitte wohne, und die Grenze dazwischen verläuft.

interessierten, sondern dies als Vorwand verwendeten, um aus politischen Gründen heimlich und rechtswidrig ein Konto auszuspionieren und zu versenken, exakt so, wie die damalige Innenministerin Faeser und der Verfassungsschutz das öffentlich angekündigt hatten, freilich ohne Rechtsgrundlage.

Ich bin daher sehr aufmerksam gegenüber Polizeimethoden, die nur unter Vorwand etabliert werden und dann für rechtswidrige, fremde, politische Zwecke missbraucht werden. Und hier sehe ich die Missbrauchsmöglichkeiten riesig wie ein offenes Scheunentor, und der Schutz gegen Missbrauch ist gleich Null.

Sie müssen sich von der Vorstellung lösen, dass die Polizei und die Staatsanwaltschaft immer „Die Guten“ wären. Das sind sie schon lange nicht mehr. In Berlin sind die Strafverfolger mitunter krimineller als die Verfolgten. Und es hat seinen Grund, warum die Polizeien anderer Bundesländer – sowohl im hier relevanten Fall der Festnahme von Daniela Klette, also auch im Fall der Juwelen aus dem Dresdner Grünen Gewölbe – die Berliner Polizei nicht mehr vorab einweißen.

11.2.2 Keine ausreichende Diskussion

In den Gesetzanträgen finden sich Brocken wie (21/8606)

Für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet öffentlich zugänglichen Daten wird daher eine ausdrückliche Rechtsgrundlage geschaffen.

Des Weiteren wird den Strafverfolgungsbehörden die Befugnis eingeräumt, zur Strafverfolgung verfahrensübergreifende Recherche- und Analyseplattformen einzusetzen. Mit dem Einsatz verfahrensübergreifender Recherche- und Analyseplattformen zur Strafverfolgung können bisher unverbundene Dateien und Datenquellen der Polizei, die sowohl die Daten aus der Gefahrenabwehr als auch aus der Strafverfolgung enthalten, in einer Analyseplattform vernetzt werden und durch Suchfunktionen systematisch erschlossen werden. Aufgesetzt werden soll auf bereits vorhandene Analyseplattformen der Gefahrenabwehr.

Das ist eine Änderung in der Strafverfolgung und Überwachung von enormem Ausmaß und unabsehbaren Folgen.

Ich glaube nicht nur nicht, dass das ausreichend erörtert wurde.

Ich glaube auch nicht, dass der Bundestag in seiner derzeitigen Zusammensetzung über die nötige Sachkunde verfügt, die Tragweite dieser Gesetze zu erkennen und zu bewerten. So findet sich ebenso in 21/8606 der Passus

Derzeit beruht die operative IT-Infrastruktur der Polizeibehörden teilweise noch auf einem unverbundenen Nebeneinander zahlreicher automatisierter Dateien und Datenquellen, die zur Strafverfolgung noch jeweils einzeln mit einem bestimmten personenbezogenen Datum abgeglichen werden müssen. Dies bindet zum einen personelle Ressourcen, zum anderen birgt dies ein Risiko von Übertragungsfehlern, Informationsverlusten oder paralleler Datenerhaltung, zumal jede neue Fragestellung erneut unter den vorangestellten Einschränkungen und Aufwänden bearbeitet werden muss (vergleiche zur Gefahrenabwehr, Drucksache des Bayerischen Landtags 19/1557, Seite 12).

Das ist zwar sachlich zutreffend. Ich glaube aber nicht, dass dem Deutschen Bundestag als Gesetzgeber die Tragweite dieser Änderung bewusst *ist* oder in seiner derzeitigen Zusammensetzung bewusst sein *kann*.

Einzig der LINKEN ist das aufgefallen – klar, wenn man mit Antifa, RAF, Hamas, Islamischem Staat verbandelt ist, achtet man dann schon auf solche Dinge, aus Eigeninteresse.

Pathologisch auffällig ist jener Satz in der Begründung

Alternativ kommt ein Verzicht auf entsprechende Regelungen in Betracht.

Damit blieben den Strafverfolgungsbehörden wichtige Ermittlungsinstrumente verwehrt, die in zunehmend digitalisierten Zeiten erforderlich erscheinen, um Straftaten weiterhin effektiv verfolgen zu können.

Ich glaube nicht, dass sie „zunehmend *erforderlich*“ sind, denn warum sollten sie erforderlicher als früher sein?

Ich glaube, dass sie „zunehmend *möglich*“ sind und Begehrlichkeiten wecken. Natürlich kann und muss der Staat auch neue Ermittlungsmethoden nutzen, wie auch schon früher Fotos, Fingerabdrücke, DNA mit deren Verfügbarkeit.

Die dazu nötige Abwägung mit den Gefahren fehlt aber völlig.

11.2.3 Angreifbarkeit vor dem Bundesverfassungsgericht

Ich halte nicht viel vom Bundesverfassungsgericht und dessen undurchsichtiger und willkürlicher Arbeitsweise. Faktisch ist das kein Gericht, sondern ein außerdemokratischer Parteienrat, dessen Tätigkeit darin besteht, die Rechtsprechung unter die Kontrolle der Parteien zu stellen.

Angesichts der Mängel dieses Gesetzentwurfs und der typischen Rechtsprechung des Bundesverfassungsgerichts halte ich die Wahrscheinlichkeit aber für begrenzt, dass diese Gesetzentwürfe Bestand haben werden. Und das auch, obwohl sie dem Zweck dienen, der Forderung des BVerfG nachzukommen.

Es wird mit Sicherheit Verfassungsbeschwerden gegen die vorliegenden Gesetzentwürfe geben, sollten sie umgesetzt werden, und diese nicht nur bei Anwendung des Gesetzes, sondern auch gegen das Gesetz selbst. Das Bundesverfassungsgericht stellt zwar sehr strenge Anforderungen an Verfassungsbeschwerden, die in der Jahresfrist unmittelbar gegen Gesetze erhoben werden. Ich könnte mir aber durchaus vorstellen, dass diese Anforderungen hier erfüllt sind, nämlich weil der Betroffene nicht informiert wird und die Ermittlungen nach dem Gesetzestext auch Personen betreffen kann, die nicht Beschuldigte sind, sondern Zeugen, Geschädigte, Unbeteiligte, und die damit weder zu rechnen brauchen, noch einen Grund zur Akteneinsicht oder das Recht dazu haben.

Sollte es tatsächlich zu einer Verfassungsgerichtsentscheidung über diese Gesetze kommen, halte ich diese *in dieser Form* für kaum zu verteidigen.

11.2.4 Mangelnde Sachkunde

Es fehlt ersichtlich an Sachkunde.

Die technischen und juristischen Begriffe sitzen nicht. „Diskriminierende Algorithmen“ ist Gefasel. Die technischen Vorstellungen sind realitätsfern und eher laienhaft.

Die Gesetzentwürfe hinterlassen den Eindruck, in völliger Praxisferne und in einem theoriegeleiteten Elfenbeinturm entstanden zu sein. Es riecht alles nach „*Das Bundesverfassungsgericht will da was haben, also schreib halt einfach irgendwas da rein, damit die zufrieden sind.*“ Eine mehr als nur oberflächliche, beamtenformale Beschäftigung mit dem Thema ist nicht ersichtlich.

Bemühen Sie sich um eine den Aufgaben adäquaten Zusammensetzung der Fraktionen und der Regierung. Und suchen Sie sich endlich jemanden, der weiß, was Algorithmen sind. Das ist ein Dauerärgernis.