



Jan Kürschner
Vorsitzender des Innen und Rechtsausschuss im
Schleswig-Holsteinischer Landtag

per E-Mail: innenausschuss@landtag.ltsh.de

Fakultät Informatik

Besucheranschrift
Esplanade 10
Gebäude B, Raum B.103
85049 Ingolstadt
www.thi.de

Prof. Dr. Tobias Eggendorfer
Professor für Sicherheit in
vernetzten Anwendungen

Tel +49 841 9348-2233
tobias.eggendorfer@thi.de

Ingolstadt, 9. September 2026

*Stellungnahme zu den Drucksachen 20/4284 und dem
Änderungsantrag der Fraktionen der CDU und Bündnis90/Grünen hierzu*

Sehr geehrter Herr Kürschner, sehr geehrte Damen und Herren,

gerne habe ich mir die Drucksachen angesehen und nehme hierzu Stellung. Ich werde vorrangig technische Aspekte betrachten, für die juristischen Fragen habe ich bereits zahlreiche, mir auch gut bekannte Kolleginnen und Kollegen in der Liste der Anzuhörenden gesehen, deren Rückmeldungen voraussichtlich umfassend sein werden.

§§184, 184a, 195a - Technische Aspekte zur Bilderkennung

Der Gesetzesvorschlag sieht eine „Echtzeit-Fernidentifikation“ anhand von Videomaterial vor.

Aus technischer Sicht ist dabei zunächst der Begriff „Echtzeit“ unpräzise: In der Informatik versteht man darunter einen Vorgang, der innerhalb einer harten Zeitobergrenze garantiert abgeschlossen wird. Diese Zeitobergrenze kann z.B. für die Auslöseentscheidung für Airbags sehr kurz sein, sie kann aber auch mehrere Sekunden oder Minuten betragen. Wesentlich ist, daß der Abschluß innerhalb dieses Zeitfensters erfolgt. Der Gesetzgeber stellt sich hier vermutlich eine „zeitnahe“ Erkennung vor und sieht das als „Echtzeit“. Dieser Begriff ist aber weder legaldefiniert noch als Ziel operationalisiert und damit nicht prüfbar.

Ich rege daher an, den Begriff „Echtzeit“ durch eine definierte Zeitvorgabe zu ersetzen. In Anbetracht der Prozessschritte, die im Anschluß folgen, kann ich mir vorstellen, daß als prüf- und meßbare Zeitvorgabe „innerhalb von weniger als einer Minute“ sinnvoll wäre.

Weiterhin muß ich in technischer Hinsicht warnen: Die technische Realität der biometrischen Gesichtserkennung ist bei weitem nicht so ausgereift, wie der Gesetzentwurf zu hoffen scheint. Für eine verlässliche Erkennung sind günstige Lichtverhältnisse, keine Verschattung wesentlicher

Merkmale wie z.B. durch Schirmmützen, Verdeckung durch Sonnenbrillen o.ä. und möglichst frontale Sicht hilfreich. Zudem ist eine Mindestauflösung der Aufnahmen erforderlich, in der Regel angegeben als Mindestanzahl von Pixeln zwischen den Augen¹, Kompression kann je nach Verfahren weitere Einschränkungen bedeuten².

Technisch lässt sich zwar argumentieren, dass durch Heranzoomen auf eine Person die nötigen Voraussetzungen geschaffen werden könnten, aber auch hier ist zu unterscheiden: Nur ein optischer Zoom, also ein durch ein Linsensystem der Kamera herbeigeführter, erreicht die nötige Bildqualität. Ein digitaler Zoom errechnet im schlechtesten Fall zusätzliche Bildpunkte abhängig von den benachbarten Punkten. Damit wird zwar für den Betrachter das Gesicht vergrößert, es ist allerdings nicht mehr die Originaldarstellung. Die aber benötigt eine biometrische Erkennung.

Praktisch bedeutet das, dass ohne optischen Zoom die Kamera nur wenige Meter vor dem Gesicht des zu Überprüfenden stehen muß. Das ist praktisch in den im Gesetzesvorschlag vorgesehenen Szenarien (öffentliche Veranstaltung, öffentlicher Raum) mit realistischem Aufwand nicht möglich. Eine solche Detektion könnte also nur im Rahmen von Zugangskontrollen zu den Veranstaltungen funktionieren.

¹ siehe u.a.: Yooyoung Lee, P. Jonathon Phillips, James J. Filliben, J. Ross Beveridge, Hao Zhang, Identifying Face Quality and Factor Measures for Video, NISTR 8004, <http://dx.doi.org/10.6028/NIST.IR.8004>, Xavier Merino, Samuel Langborgh, Gabriella Pangelinan, Michael King, Reading Between the Eyes: Assessing the Impact of Interpupillary Distance on Face Recognition, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10971699>, Hyun-Cheol Choi, Unsang Park, and Anil K. Jain, PTZ Camera Assisted Face Acquisition, Tracking & Recognition, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5634539>, Mohamad Firham Efendy Md Senan, Siti Norul Huda Sheikh Abdullah, Wafa Mohd Kharudin, Nur Afifah Mohd Saupi, CCTV Quality Assessment for Forensics Facial Recognition Analysis, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7943232>, Christian Herrmann, Chengchao Qu, Dieter Willersinn and J'urgen Beyerer, Impact of Resolution and Image Quality on Video Face Analysis, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7301750>

² Brendan Klare, Mark Burge, Assessment of H.264 video compression on automated face recognition performance in surveillance and mobile video scenarios, SPIE Defense + Security, 2010, Orlando, Florida, United States, Volume: Biometric Technology for Human Identification VII; 76670X (2010), <https://doi.org/10.1117/12.851349>

Soweit die Vorstellung besteht, daß mit „künstlicher Intelligenz“³ Vorteile erzielt werden könnten: Auch die setzt die physikalisch-technischen Grundlagen nicht außer Kraft. Fehlende Bildinhalte kann auch künstliche Intelligenz nicht verlässlich und korrekt ersetzen, geschweige denn zur Erkennung nutzen.

§§184, 184a, 195a - Nutzung von Künstlicher Intelligenz

Über die technischen Beschränkungen hinaus, ist dringend anzuraten, soweit „künstliche Intelligenz“ zum Einsatz kommen soll, diese auf eigenen Systemen zu nutzen. Das heißt, die erforderlichen Daten an Anbieter außerhalb des Einflusses des Grundgesetzes zu übertragen, könnte erhebliche Risiken für die Betroffenen bedeuten.

Der „Hacking“-Vorfall in der Berliner Senatsverwaltung ist insoweit ein deutliches Beispiel, der umfangreich personenbezogene Daten öffentlich gemacht hat. Sowohl der Verlust identifizierender biometrischer Daten als auch der Videoaufnahmen können die persönliche Sicherheit der Betroffenen erheblich beeinträchtigen.

Die Cyber-Täter differenzieren dabei nicht zwischen den personenbezogenen Daten von Straftätern oder möglichen Bewegungsprofilen von z.B. Landesbeamten. Täter könnten erzeugte Videos gegen deren aus dem Internet gewonnene Bildmaterialien abgleichen und somit auch z.B. verdeckte Ermittler aufklären. Das insoweit für Ermittlungsbehörden vorgesehene Verbot im Gesetzesentwurf interessiert sie nicht.

Auf die Grenzen, die die EU KI-Verordnung insoweit setzt, insbesondere, daß es sich hier voraussichtlich um eine KI höchster Risiko-Klasse handeln dürfte, wird hingewiesen⁴.

Anzumerken ist auch, daß der Abgleich von biometrischen Daten weder KI erfordert, noch ersichtlich eine sinnvolle Anwendung von KI ist. Eine Lösung ohne KI wäre einfacher in eigener Regie zu betreiben, damit cyber-souverän, und weniger energieaufwendig. Rechtliche Beschränkungen durch die KI-VO entfielen dann, es blieben u.a. die durch die DSGVO.

§§184, 184a, 195a - Kontrolle durch Menschen

Zu beachten ist, dass KI-Verfahren stets nur Wahrscheinlichkeiten als Ausgaben erzeugen, ein KI-generierter Treffer also kein sicherer Match ist. Der Gesetzgeber sieht hierzu vor, dass ein Mensch die Meldung vor Maßnahmen zu prüfen habe. In anderen Umgebungen, beispielsweise bei der Evaluation

³ „künstliche Intelligenz“ (KI) beschreibt nicht eine Technologie, sondern eine Menge von Verfahren unterschiedlicher Komplexität, die letztlich basierend auf Wahrscheinlichkeiten Aussagen treffen. Daher ist der Begriff hier in Gänsefüßchen gesetzt. Insbesondere derzeitige Verfahren sind nicht im üblichen Wortsinn „intelligent“, sie wirken nur nährungsweise für den Nutzer so. Tatsächlich reproduziert KI nur Bekanntes und präferiert dabei besonders Wahrscheinliches.

⁴ Matthias Eichfeld, KI-Gesichtserkennung im Fußballstadion – Möglichkeiten und Grenzen nach KI-VO und Datenschutzrecht, Tagungsband der DSRI-Herbstakademie 2026

von Kreditwürdigkeiten, zeigt sich regelmäßig, dass zwar auf dem Papier ein Mensch an der Entscheidung beteiligt wird, allerdings sind der Aufwand und die wahrgenommene Verantwortung, um von der vorgeschlagenen Computer-Entscheidung abzuweichen, für den Menschen so hoch, dass regelmäßig die Computerentscheidung bestätigt wird. Damit findet aber faktisch keine Kontrolle mehr statt.

Daher sollte der Gesetzgeber - soweit er an dem Verfahren festhält - die Hürde zur Bestätigung genauso hoch ansetzen, wie die Hürde zur Ablehnung der Computer-Entscheidung. Das kann zum Beispiel dadurch erfolgen, daß der Mensch sowohl die Bestätigung als auch Ablehnung begründen muß und der Begründungsumfang jeweils mindestens gleich lang ist, etwaig vorgegebene Textbausteine beide Situationen gleich gut abdecken, und so keine Präferenz in eine Handlungsalternative schaffen.

Auch sollten die menschlichen Prüfer in beide Richtungen in gleichem Maße in der Verantwortung für ihre Entscheidung stehen. Auch das lässt sich durch organisatorische Maßnahmen, wie z.B. einer verbindlichen Fehleranalyse mit dem Vorgesetzten bei Fehlentscheidungen im Nachgang erreichen.

§184 (5) - Identifikation von Handlungen

Der Gesetzentwurf sieht ein automatisiertes Erkennen von Handlungen vor, die u.a. die sexuelle Selbstbestimmung oder das Leben beeinträchtigen können. Eine solche Erkennung dürfte technisch derzeit noch nicht mit einer über Zufall hinausgehenden Verlässlichkeit möglich sein, wie sich auch in Mannheim und Berliner Südkreuz andeutet⁵.

Das lässt sich auch technisch gut nachvollziehen: Den Humpelnden, der sich stützt, vom Alkoholisierten, der sich stützt, zu unterscheiden, dürfte genauso komplex sein, wie ein freiwilliges Paar von einem unfreiwilligen zu unterscheiden. Die Reaktionen Betroffener von Gewalttaten und wahrgenommener Bedrohung divergieren so erheblich, dass sich menschliche Beobachter bereits schwer tun, die Situationen einzuordnen. Genau deswegen gibt es mittlerweile Handgesten, mit denen Betroffene unauffällig auf ihre Situation aufmerksam machen können

Die Idee, durch Schauspieler Situationen vorzuspielen, und so ein System zu trainieren, wirkt zwar plausibel, ist aber angesichts der unzureichenden Trennschärfe und der Vielzahl an möglichen Szenarien nicht zielführend.

§184 (6) - Speicherung von Daten

Der Ansicht dieses Gesetzentwurfes, die erhobenen Daten dürfen nicht gespeichert werden, spricht die Interpretation u.a. des Urheberrechts entgegen, die auch schon eine Zwischenspeicherung als Vervielfältigung eines Werkes sieht: Das mag zwar im Einzelfall eine harte Auslegung sein, aber eine, der technischen Natur entspricht. Naturgemäß müssen Daten zur Verarbeitung gespeichert werden.

⁵ <https://netzpolitik.org/2026/verhaltenserkennung-in-mannheim-10-000-filme-fuer-ein-hallelujah/>,
<https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz>

Computer können nur auf einem Speicher Daten verarbeiten. Ohne Speicherung ist schlicht kein Abgleich möglich.

Der Gesetzgeber könnte vorgeben, dass die Speicherung nur im flüchtigen Arbeitsspeicher erfolgen darf und müßte vorgeben, daß dann auch keine Auslagerungsspeicher (Swap-Speicher) zu nutzen sind. Dann wäre zumindest die Speicherdauer beschränkt, der Speicherinhalt spätestens beim Ausschalten verloren und je nach Dimensionierung des Arbeitsspeichers auch damit zu rechnen, dass der Speicher wahrscheinlich nach einer bestimmten Zeitspanne überschrieben ist.

Soweit nicht nur im Arbeitsspeicher gearbeitet wird, sondern auch eine Zwischenspeicherung auf Datenträgern wie Festplatte oder Solid-State-Disk erfolgt, müßte der Gesetzgeber nicht nur eine Löschung, sondern eine forensisch sichere Lösung fordern.

In beiden Fällen könnten Angreifer jedoch, wenn sie Zugriff auf das System erlangen, zumindest die „Live-Daten“ abgreifen. Nach dem aktuellen Stand der Qualität von Software sind solche Vorfälle als durchaus plausibel und zu erwarten einzustufen.

§184b (1), §195 (2) - Pass- und Ausweisdaten

Es bleibt unklar, ob die „im Rahmen der polizeilichen Arbeit“ erlangten Daten auch die biometrischen Daten von Pässen und Ausweisen umfasst. Die Eingriffsintensität würde deutlich erhöht, wären diese Daten mit erfasst, im Vergleich zu z.B. im Rahmen von erkennungsdienstlichen Maßnahmen erfassten Daten.

Diese Unklarheit sollte im Rahmen der Gesetzgebung geklärt werden.

§§188c, 188d automatisches Zusammenführen und Auswerten

Es entsteht der Eindruck, dass das automatische Zusammenführen und Auswerten von Daten über Personen auch mit KI erfolgen soll. Dabei wiederhole ich meinen Hinweis auf die Grenzen von KI von oben, die nur Wahrscheinlichkeiten aufgrund von vorigen Trainingsdaten liefern kann. Sie kann damit zwar möglicher Weise unterstützen, aber auch Fehlinformationen liefern.

Zudem kann in vielen KI-Systemen von Drittanbietern, entgegen deren eigenen Behauptungen, nicht sichergestellt werden, dass die Löschansprüche auch umgesetzt werden. Wenn man überhaupt solche Lösungen möchte, dann wäre es dringend anzuregen, in Deutschland geeignete Verfahren seriös zu erforschen und zu entwickeln, um sie selbst zu betreiben.

Soweit der Gesetzesentwurf nachvollziehbare KI-Entscheidungen fordert, begrüße ich das zwar, weise aber darauf hin, daß die bundeseigene Agentur für Innovation in der Cybersicherheit, die Forschung mit einem hohen Risiko des Scheiterns beauftragt, die im Erfolgsfall in 5-10 Jahren einen Technology Readiness Level von 4-5, also einen Laborprototypen, hervorbringt, gerade erst ein großes Forschungsprojekt zu „erklärbarer KI“ angestossen hat. Projekte, die die Agentur anstösst, werden zunächst von BMI und BMVg umfangreich auf Parallelforschung geprüft. Mithin ist davon auszugehen,

dass es aktuell niemand gibt, der seriös und ohne kreative Umdeutung des Begriff erklärable und nachvollziehbare KI-Systeme anbieten kann.

Die vorgesehene gesetzliche Vorgabe ist also nach derzeitigem Stand der Technik nicht erfüllbar. Mit den üblichen Vorgaben der Cyberagentur lässt sich auch gut begründen, daß mit einem Prototypen nicht vor in frühestens 5-10 Jahren zu rechnen ist, Marktreife dann üblicher Weise nochmals mehrere Jahre braucht.

§195b (1) - Nachträglicher Abgleich - Echtzeit

In §195b (1) findet sich wieder die unklare Verwendung des Begriffs „Echtzeit“. Generell sind in technischer Hinsicht die Übertragungsprotokolle des Internets sämtlich nicht echtzeitfähig. Sie bieten keine harte Zeitobergrenze, sondern übertragen nach einem Best-Effort. Damit wären bei technischer Auslegung auch Video-Live-Streams für die Auswertung zulässig.

Der Gesetzgeber müßte hier den Begriff „Echtzeit“ für den Anwendungszweck definieren, klüger wäre ein eigener Begriff, um Verwechslung vorzubeugen.

In technischer Hinsicht bleibt unklar, warum ein Live-Stream unzulässig sein soll, wohingegen zum Beispiel ein von Dritten gefertigter Screenshot eines Live-Streams, der zum Download angeboten wird, zulässig sein soll. Die enthaltenen biometrischen Daten sind identisch.

Unklar ist auch, ob z.B. aus einem typischer Weise stattfindenden Buffering eines Live-Streams entnommene Daten - weil die nun technisch sicher keine Echtzeitdaten mehr sind - möglicher Weise zulässig sein könnten.

§195b - Eingriffsintensität

Ohne das vertiefen zu wollen, weil ich davon ausgehe, daß die angefragten Stellungnahmen der juristischen Kolleginnen und Kollegen hierauf kritisch eingehen werden, ist die Vorstellung, im Internet massenhaft Bild-, Video- und Audiodaten abzusammeln, und diese dann abzugleichen, ein massiver Eingriff in die Grundrechte.

In technischer Hinsicht ist die geplante Maßnahme äußerst aufwendig: Denn entweder müßte eine Sammlung aller Bilder im Internet, die eine Person zuordnungsfähig enthalten, gefertigt werden, aus dieser die biometrischen Daten der Personen extrahiert werden, die Bilder den Personen zugeordnet werden - um dann bei einer Suche mit einem effizienten Algorithmus durch die gigantische Datenmenge durchzugehen, um in biometrischen Merkmalen übereinstimmende Personen zu finden. Die erforderlichen Datenmengen sind erheblich, die Suchaufwände auch mit effizienten Algorithmen gigantisch.

In der Gegenrichtung könnte man mit den biometrischen Daten eines Verdächtigen das Internet durchkämmen und alle Bilder abgleichen. Doch auch das kostet erheblich Rechenaufwand und Bandbreite: Es muß jedesmal das komplette Netz abgesucht werden, aus jedem Bild biometrische

Features extrahiert werden und die abgeglichen. Hier ist zwar der Speicheraufwand kleiner als in der ersten Lösung, aber dafür der Suchzeitaufwand höher.

Beide Ansätze erscheinen nach dem Stand der Technik nicht vernünftig implementierbar für ein Bundesland. Es müßte sich dazu eines externen Dienstleisters bedienen. Die, die in Ansätzen (!) solche Leistungen derzeit anbieten, können aber keine belastbaren Konzepte vorlegen, wie sie die Daten der Betroffenen schützen und eine Unschuldsvermutung garantieren.

§179 (6) i.d.F. des Änderungsantrages

Wer den Notruf wählt, steht im Allgemeinen in einer Ausnahmesituation und daher gestresst. Oft wissen Opfer oder Helfer nicht genau, wo sie sich befinden. Der Regelungsvorschlag ist diesbezüglich hilfreich: Die Polizei sieht den Standort sofort. Das spart Zeit und kann Leben retten. Dieser Ansatz ist wichtig, richtig und sinnvoll. Entsprechende Lösungen finden sich auch schon in einigen Rettungsleitstellen. Sie erleichtern die Notrufabfrage, die Zuordnung der Einsatzstelle und helfen so, zügig zu helfen.

Doch der Vorschlag vergisst Menschen, die unerkannt bleiben wollen oder zu ihrem eigenen Schutz müssen. Aussteiger, Informanten oder Tatbeteiligte melden Verbrechen nur ohne Risiko. Wenn das System ihren Standort automatisch erfasst, schweigen sie aus Angst. Das kann Chancen vergeben. In einigen Polizeipräsidiien gibt es daher bereits anonyme, telefonische Kontaktmöglichkeiten. Hinweisgeberportale erfüllen diesen Zweck nicht, da sie nicht in der akuten Situation nutzbar sind.

Der Gesetzgeber muss den Entwurf nachbessern. Anrufer müssen verhindern können, z.B. durch eine gesonderte, anonyme Notrufnummer, dass das System ihren Aufenthaltsort ausliest. Nur ein anonymer Notruf schützt auch diese Hinweisgeber. Es trägt auch dazu bei, den „nemo tenetur“-Grundsatz umzusetzen.

§184d i.d.F. des Änderungsvorschlages

Die Vorstellung in dem Änderungsvorschlag, Computersysteme könnten abgelenkte Autofahrer erkenne, ist schlicht falsch: Bisherige Experimente und auch tatsächlich implementierte Systeme weltweit haben gezeigt, daß die Erkennungsrate bestenfalls Zufallsniveau erreicht. Damit stellt sich zunächst die Frage: Welchen Nutzen hätte der Änderungsvorschlag?

Vermutlich ist es kosteneffizienter, zusätzliche Polizeibeamte zu ernennen, und die mit einer Verkehrsüberwachung zu beauftragen. Die erhöhte Polizeipräsenz zeigt zumindest belegt eine positive Wirkung auf Verkehrsteilnehmer, wirkt nebenbei kriminalpräventiv und ist anders als eine Fernüberwachung auch in der Lage, sofort zu intervenieren.

Statt also bekannt wirkungslose Systeme zu codifizieren, teure Experimente mit absehbar schlechten Erfolg durchzuführen, wäre eine Investition in das Personal der Polizei sinnvoll.

§185 (2) i.d.F. des Änderungsvorschlages

Der Änderungsvorschlag strotzt in Nr. 2 von unterdefinierten und / oder nicht prüfbaren Rechtsbegriffen. Ein „absehbarer Zeitraum“ entzieht sich einer konsistenten richterlichen Prüfung, statt konkrete Zeiträume zu benennen oder zumindest prüfbar zu machen. Auch ist die Menge der Taten, die zu der Überwachung berechtigen, nicht konkret benannt. Ohne den Katalog des §100a (2) StPO dabei zur Maßgabe für die schweren Taten machen zu wollen, so zeigt er jedoch, wie handwerklich korrekt Nachprüfbarkeit entsteht.

§185a i.d.F. des Änderungsvorschlages

§100a StPO enthält eine Regelung zur Telekommunikationsüberwachung im Ermittlungsverfahren. Es bleibt unklar, wieso sich der Polizei Schleswig-Holstein nun auch Telekommunikationsüberwachung für die Gefahrenabwehr in das Gesetz geschrieben werden soll. Denn der Änderungsvorschlag knüpft Tatbestände an die Überwachung, die ausreichen, um ein Ermittlungsverfahren zu begründen und damit über §100a StPO Zugriff zu erhalten.

Aus hiesiger Sicht kann dieser Vorschlag daher gestrichen werden, der Nutzen ist gering, die Wahrscheinlichkeit, dass er einer verfassungsgerichtlichen Prüfung nicht standhält hoch.

§185b i.d.F. des Änderungsvorschlages

Die Zielsetzung des Änderungsvorschlages ist nachvollziehbar: Einem Straftäter soll ein Kommunikationsmittel entzogen werden, das kann in Notfällen auch sinnvoll sein - eine über das Handynetz ferngesteuerte Drohne mit Sprengsatz wäre so ein Fall. In solchen Fällen ist auch nachvollziehbar, das Gefahrenabwehrrecht zu bemühen, anders als in §185a i.d.F. des Änderungsvorschlages.

Der Vorschlag allerdings referenziert auf §185a. Ich rege daher an, hier tatsächlich einen nachvollziehbaren Maßnahmenkatalog für Notlagen, die einen solchen Eingriff begründen sollen, in §185b vorzusehen.

§185e i.d.F. des Änderungsvorschlages

Der Änderungsvorschlag ist völlig unspezifiziert: Mobile Sensorsysteme können beliebige Daten erfassen, von der Luftfeuchte und Temperatur über Lautstärke und ggf. Sprechinhalte bis hin zum Einsatz eines mobilen Gas- oder Sprengstoffspürsystems. In dem Kontext und Gesamtduktus dieses Änderungsvorschlages vermute ich zwar, dass z.B. IMSI-Catcher und „Sensoren“ für MAC-Adressen von WLAN- und Bluetooth-Adaptoren zum Einsatz kommen könnten, um so Handys, Smartwatches etc. zu identifizieren und zu tracken. Doch das ist eine Hypothese.

Als handwerkliches Minimum eines Gesetzesvorschlages wäre zu erwarten, dass der geplante Eingriff so genau benannt ist, daß er zumindest verfassungsrechtlich prüfbar wird, und erläutert ist, welche Zwecke der Eingriff verfolgt. Denn auch das ist hier allenfalls zu erahnen.

Auch ein reines Tracking von Handys und Wearables, das hier mutmaßlich gedacht sein könnte, ist übrigens grenzwertig: Es greift gerade bei Veranstaltungen unter Umständen tief in den höchstprivaten Lebensbereich ein: Man denke an den berühmten Keraschwenk der „Kiss-Cam“ bei einem Coldplay-Konzert in Boston oder stelle sich Teilnahmen an an gewerkschaftlichen Kundgebungen oder Veranstaltungen wie dem Christopher Street Day vor, die immer noch Diskriminierungen auslösen können.

Anmerkungen zum Änderungsvorschlag insgesamt

Der Änderungsvorschlag, insbesondere die in vorherigen Abschnitten diskutierten Punkte mit Ausnahme des §179 (5), gehen weit über das hinaus, was Inhalt des ursprünglichen Gesetzesvorschlages war. Nach hiesiger Auffassung, die sich voraussichtlich auch in den Stellungnahmen der juristischen Kollegen wiederfinden wird, bestehen ernstliche Zweifel, wie diese Vorschläge mit dem Grundgesetz in Einklang zu bringen sind.

Kontrolle über KI

Zwar besteht derzeit anscheinend die Ansicht, alle Probleme der Welt durch KI lösen zu können - früher sollten Big Data und Data Lakes das schaffen, so treiben die Phantasien neue Entwicklungen der Informatik konstant zu unglaublichen Wundermitteln auf. Unbeschadet dieser Vorstellung: Die aktuelle Entwicklung in der Welt zeigt, daß der Einsatz von IT-Systemen außerhalb der eigenen Kontrolle besondere Gefahren birgt: Der internationale Strafgerichtshof mußte erfahren, daß eine von der US-Regierung als politisch unerwünschte Untersuchung zum Abschalten des Microsoft-Zugangs führen kann, in den USA werden extensiv Daten von Palantir mißbraucht (nach deutschem Verständnis), um Einwanderer förmlich zu jagen. Es gibt auch durchaus intensive Diskussionen über politische Nähe von Palantir zu unerwünschten Gruppierungen.

Trotzdem deuten einige Formulierungen im Gesetzesvorschlag deutlich daraufhin, daß deren Überwachungs- und Kontrollsoftware die Blaupause für die angestrebten Verfahren liefert. Das erscheint durch die Technikgestaltung gefährlich. Es entsteht eine umfassende Abhängigkeit von einem US-Anbieter, der nach Gutdünken der dortigen Regierung agieren muß, und gleichzeitig eine völlig unklare Datenweitergabesituation.

Selbst wenn man - anders als ich mit den obigen Argumenten - zu dem Ergebnis kommen sollte, daß die Vorstellungen des Gesetzesvorschlag oder gar des Änderungsvorschlages in ihrer Gänze notwendig, verfassungskonform und sinnvoll sein sollten, so bleibt der Wunsch an den Gesetzgeber, explizit vorzuschreiben, dass ausschließlich in der EU entwickelte und betriebene Lösungen zum Einsatz kommen. Nötigenfalls möge das Land dafür Forschungsmittel bereitstellen und so die Wissenschaft in Europa oder auch ausschließlich Schleswig-Holstein stärken. Damit investiert das Land in eine cyber-souveräne, -resiliente Zukunft. Das ist aktuell dringend geboten.

Anonymität als wichtiger Schutzfaktor im Alltag

Wir schützen Menschen regelmäßig durch Anonymität. So gibt es anonyme Drogenberatung, psycho-soziale Beratungsstellen, AIDS-Tests etc. Beispielsweise die Münchner Insel, eine solche anonyme, psycho-soziale Beratungsstelle, hat ihre Räume bewußt im Zwischengeschoß des Münchner U-Bahnhofs Marienplatz, vermutlich einer der stärkst frequentierten. Das soll Ratsuchenden ermöglichen, die Insel anonym aufzusuchen, das soll Zugangsbarrieren abbauen.

Müßten Klienten nun damit rechnen, dabei durch polizeiliche Maßnahmen erfasst zu werden, würde das die Nutzbarkeit der Beratungsstelle erheblich reduzieren. Die Hemmschwelle steigt.

Arztgeheimnis, Mandatsgeheimnis etc., deren Verletzung §203 StGB unter Strafe stellt, das u.a. in §53 StPO besonders geschützt ist, sind hohe Rechtsgüter. Zu diesen schützenswerten Geheimnissen gehört auch, wer wann einen Geheimnisträger besucht. Eine Videoüberwachung, die biometrische Daten erfasst und abgleicht, unterläuft diesen Schutz.

Es müßten also explizit Überwachungsschutzräume in einem so großen Umkreis um entsprechende Stellen eingerichtet werden, dass auch durch Korrelation von Daten nicht ersichtlich ist, ob der Beobachtete sich in einer solchen Einrichtung aufgehalten hat.

Regierungen mit anderem Verhältnis zur Demokratie

Das Landesamt für Verfassungsschutz Sachsen-Anhalt hat erhebliche Zweifel an der Verfassungstreue der dort nun mehrheitlich in den Landtag gewählten AfD geäußert. Ebenso gibt es in USA seit den letzten Wahlen einen Präsidenten, dessen Haltung zur Demokratie weltweit Zweifel weckt. Unabhängig davon, wie wohl- oder schlechtmeinend solche Regierungen sein können: Eine heute aufgebaute Infrastruktur kann von nicht-demokratischen Regierungen und Regimes mißbraucht werden. Ein aktuelles Beispiel ist der Mißbrauch einer Einwanderer-App in den USA durch ICE. Technologien, die wir heute etablieren, müssen daher vor Übergriffen durch potentiell verfassungs- oder demokratiefeindliche Regimes geschützt werden.

Ich hoffe, Ihnen durch diese Stellungnahme hilfreiche Impulse gegeben zu haben, stehe gerne für Rückfragen zur Verfügung und würde mich freuen, wenn ich durch meine Rückmeldung einen Beitrag zur Weiterentwicklung des Rechts in Schleswig-Holstein leisten konnte.

Mit freundlichen Grüßen

Prof. Dr. Tobias Eggendorfer