Deutscher Bundestag Drucksache 20/4200: Menschenschutz versus Datenschutz

GISAD

„Trusted WEB 4.0 ist die Integration aller über das Web verfügbaren Ressourcen in ein Gesamtsystem.

Maschinen, Geräte und Menschen sind global erreichbar, in dezentralisierten, anonymisierten Strukturen organisiert.

Trusted WEB 4.0 bildet vordigitale Gesellschaftsstrukturen ab.

Die Wertschöpfungsketten werden neu organisiert.“

GISAD Global Institute for Structure relevance, Anonymity and Decentralization i.G.
EU Transparency Register Nr. 244298340978-40

Webseite: www.gisad.eu

Krefeld, Deutschland, 1. Fassung den 2. Dezember 2022

Die Zitate beziehen sich auf die Drucksache 20/4200 soweit nicht andere Quellen genannt sind.

Alle Definitionen zum Menschenschutz wurden von mir erstellt.

Stellungnahme zur Drucksache 20/4200 des Deutschen Bundestags: Digitaler Menschenschutz versus Datenschutz.

Inhalt

1 Vorwort

Seit nunmehr 30 Jahren beschäftige ich mich mit der Digitalisierung.

1970 bereits gab es das erste Datenschutzgesetz in Hessen. Der damalige hessische Ministerpräsident Albert Osswald anlässlich der Verabschiedung des Gesetzes:

> *„Die Orwellsche Vision des allwissenden Staates, der die intimsten Winkel menschlicher Lebenssphäre ausforscht, wird in unserem Land nicht Wirklichkeit werden."*

Niemand kann also behaupten, man hätte die durch die Digitalisierung entstehende Probleme nicht rechtzeitig erkannt.

Umso überraschender ist es, dass bis heute in der Digitalisierung faktisch nicht der Mensch im Mittelpunkt der Betrachtung steht, sondern immer im Nachhinein durch neue IT-Entwicklungen entstandene Datenprobleme mit Persönlichkeitsrechten über neue Gesetze geregelt werden.

Seit über 50 Jahren geht die politische Diskussion mal in die eine und mal in die andere Richtung. So funktioniert Demokratie. Nicht berücksichtigt wurde jedoch, dass man im Nachhinein bereits entstandene technische Besitzstände und Monopole nur noch schwer regeln oder sogar rückgängig machen kann. Insofern gibt es immer einen Schritt in die richtige Richtung und zwei Schritte zurück. Spätestens der Twitter-Kauf durch Elon Musk sollte dem letzten klarmachen, dass der Staat aktiver seine vordigitalen Rechte und Pflichten ins Digitale übernehmen muss. Es kann nicht sein, dass ein Monopolist entscheidet, welcher Politiker in der Demokratie was sagen darf. An anderer Stelle habe ich schon eine faktische Selbstzensur der Medien bewiesen, wenn es um Themen zum Erhalt der Demokratie geht. Die sich verändernden technischen Möglichkeiten der Torwächter lassen sich nicht nachhaltig in Gesetze gießen. Torwächter sind nichts Anderes als Überwacher im rechtsfernen Raum. Sowohl Torwächter als digitale Monopolisten als auch Autokratien wollen Massen steuern. Global Player nehmen auf Autokratien Rücksicht, wie gerade durch Apples Einschränkung von AirDrop auf Wunsch von China bestätigt. Hier wird eine dezentrale Funktion, die dem Nutzer einen Teil seiner Verfügungsgewalt zurückgibt beschnitten, ohne dass die Nutzer und demokratischen Staaten ein Mitspracherecht hätten.

Demokratie in der digitalen Gesellschaft kann nur in einer digitalen Infrastruktur für die Daseinsvorsorge in Hoheit der Demokratien gesichert werden. Das von mir vorgeschlagene EU-D-S (Europäisches-Digital-System) bietet die Basis zur Entwicklung einer solchen Infrastruktur. Nach den Versäumnissen der öffentlichen Hand und dem hierdurch jahrelang unterdrückten Markt für digitale Produkte zum Demokratieerhalt darf nicht erwartet werden, Unternehmen zu finden, welche sich ohne besondere Anreize betätigen. Vielmehr sind sogar für Nutzer Anreize zu schaffen, Demokratie erhaltend sich in eine entsprechende Infrastruktur aktiv einzubringen. Über 90 Stellungnahmen zu EU-Initiativen als ganzheitlichem digitalem Marschallplan sind unter https://gisad.eu/statements/ zu finden.

Viele personalisierte und pseudonymisierte Anwendungsbereiche werden wie bisher bestehen bleiben. Für viele anderen Anwendungsbereiche ist es aus Sicht des Menschenschutzes sinnvoller, wenn nur im Einzelfall und nach richterlicher Verfügung eine Personalisierung erfolgen kann, grundsätzlich jedoch persönliche Daten nicht im WAN (Wide Area Network) gespeichert sind. Hierbei

spreche ich im Folgenden von WAN-Anonymität. Nur in manchen Fällen wird es aus Sicht des Bürgers sinnvoll sein, über eIDAS eine sofortige eindeutige Identifikation herzustellen.

Auch vorhandene Datenbestände müssen verwaltet werden. Datenschutz und die DSGVO sind sinnvoll, solange persönliche, personalisierte, pseudonymisierte oder anonymisierte Daten verwendet werden. WAN Anonymität muss datentechnisch so sicher gestaltet werden, dass sie von den Anforderungen der DSGVO nicht betroffen ist.

Das EU-D-S soll als zusätzliches System für den Menschenschutz eingeführt werden. Ich behaupte, dass die beteiligten Akteure es bisher fahrlässig versäumt haben, sich um den digitalen Menschenschutz zu kümmern.

Hierfür habe ich den digitalen Menschenschutz wie folgt definiert:

Digitaler Menschenschutz erfasst die vordigitalen demokratischen Rechte und Pflichten der Bürger und optimiert sie mit den Möglichkeiten digitaler Technik.

Das Verhältnis von Technik und Werten definiere ich dabei so:

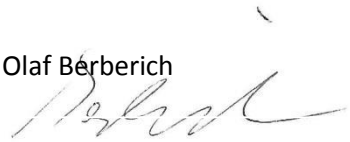
Werte entwickeln sich über viele Jahre in einem demokratischen Prozess. Technologie entwickelt sich in immer kürzeren Zyklen weiter.

Ziel des Menschenschutzes ist der Erhalt von Werten und eine Verlässlichkeit der Systeme für die Bürger, die möglichst alle digital eingebunden werden.

Jede technische Innovation ist daraufhin zu überprüfen, ob sie die Werte erhält und für die Bürger einen echten Mehrwert bietet.

Diese Stellungnahme zur Technikfolgeabschätzung von Beobachtungstechnologien bietet eine willkommene Möglichkeit, um zu beweisen, dass bisher der Menschenschutz weitgehend unberücksichtigt bleibt.

Olaf Berberich



2 Vergleich der Herangehensweisen

2.1 Vorbemerkung

Diese Stellungnahme wurde von mir alleine und auf eigene Kosten verfasst. Entsprechend kann sie keinen Anspruch auf Vollständigkeit oder das Darstellen einer Komplettlösung erheben. Basis sind jahrelange Vorarbeiten unter anderem mit der Anmeldung von eigenen Patenten, siehe https://komon.de/patentanmeldungen/ . Es wird nicht zwingend davon ausgegangen, dass genau meine Technologieideen für den digitalen Menschenschutz eingesetzt werden.

Ziel dieser Stellungnahme ist es, ausreichend Anhaltspunkte für den Beweis zu schaffen, dass bisher keine Produkte zum digitalen Menschenschutz entwickelt wurden. An anderer Stelle habe ich ausgeführt, warum diese Demokratie gefährdende technologische Einbahnstraße von den beteiligten Akteuren eingeschlagen wurde, siehe https://gisad.eu/de-alle-fuer-eine-eu-eine-analyse-zu-ueber-50-eu-initiativen/ , schon weil diese in einem globalen Markt sowohl für Demokratien als auch für Autokratien kompatibel sein wollen.

2.2 Systeme für den Datenschutz

> *„Im TAB-Bericht werden die wissenschaftlich-technischen Grundlagen der jeweiligen Beobachtungstechnologien in Abhängigkeit von den Einsatzanforderungen und -bedingungen, der erwartete und der tatsächliche Sicherheitsnutzen der jeweiligen konkreten Einsatzpraktiken, die rechtlichen Rahmenbedingungen und die aktuellen Einsatzpraktiken sowie mögliche nichtintendierte Wirkungen und Folgen des Technologieeinsatzes auf die beobachteten Personen und die Sicherheitsakteure analysiert.“*

Dieser Auszug aus dem Vorwort der Drucksache 20/4200 weist auf das Vorgehen zum Datenschutz hin:

- Im ersten Schritt geht es um die konkreten, aktuellen Einsatzpraktiken von Beobachtungstechnologien.
- Im zweiten Schritt geht es um wissenschaftlich-technische Grundlagen und den tatsächlichen Sicherheitsnutzen und rechtliche Rahmenbedingungen.
- In einem dritten Schritt erst geht es um mögliche Schäden durch nichtintendierte Wirkungen.

> *„Auf dieser Grundlage werden Gestaltungsoptionen vorgestellt, die zu einem zielführenden und gesellschaftlich tragfähigen Umgang mit Beobachtungstechnologien für zivile Sicherheitsaufgaben beitragen können.“*

- Erst in einem vierten Schritt geht es um ein gesellschaftlich tragfähiges Konzept.

Für den Bürger weitgehend undurchsichtig ergibt sich eine Gemengelage einerseits aus Interessen meist international -also auch in Autokratien- skalierenden IT Unternehmen und Behörden andererseits.

Es dient der Monopolbildung großer Unternehmen, wenn ihre Systeme möglichst komplex und umfassend sind. Einen solchen Umfang können kleinere Unternehmen nicht anbieten. Die Komplexität erschwert es, den möglichen Missbrauch von Daten zu erkennen.

Ohne böse Absichten zu unterstellen, entwickeln Menschen einen Tunnelblick, welche beruflich die schwere Verantwortung tragen, für die Sicherheit in der Gesellschaft verantwortlich zu sein.

Sicherheitsbehörden wünschen sich eine totale Überwachung, schon um eigenes Fehlverhalten und hieraus resultierende Nachteile für sich auszuschließen.

> *„Die Inhalte des TAB-Berichts bieten eine umfassende Sachgrundlage für die politische Meinungsbildung bezüglich der erforderlichen Rahmensetzung für den Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit.“*

- Erst im 5. Schritt geht es um die politische Meinungsbildung.

Noch deutlicher könnte man die Ursache nicht beschreiben, warum die Gesetzgebung immer komplexer wird, warum die DSGVO in vielen Fällen unnötig eine gesellschaftlich akzeptierte Datenverwertung einschränkt, warum selbst die meisten Profis sich heute in vielen Fällen mit der Rechtsauslegung überfordert fühlen und letztendlich die verfassungsgemäße Ordnung in der digitalen Transformation auf der Strecke bleibt!

Auch der TAB-Bericht verschließt sich dieser Kritik nicht grundsätzlich: (7.3.2 S216) „Die verfassungsrechtliche Geeignetheitsprüfung reduziert sich insofern im Wesentlichen auf einen Nachweis der technisch-funktionalen Eignung der jeweiligen Beobachtungstechnologie. Über den tatsächlichen Nutzen des Technologieeinsatzes für die Kriminalitätsbekämpfung sagt dies allerdings noch sehr wenig aus.“

2.3 Systeme für den Menschenschutz

Ich präsentiere hier nicht meine Idee, sondern ein Vorgehen, welches sich ohne die Steuerung durch meist noch nicht einmal europäische IT Firmen logisch anbieten würde. Auch beantworte ich eine Frage des TAB-Berichts: (7.3.2 S216) „Es stellt sich die Frage, wie die Möglichkeiten für den Gesetzgeber, Aussagen zur Geeignetheit neuer polizeilicher Beobachtungspraktiken zu treffen, verbessert werden können.“ Die Antwort ist einfach, die Beobachtungspraktiken müssen vom Bürger her gedacht werden!

Dafür setze ich den 5. Schritt an erste Stelle. Wobei die politische Meinungsbildung weitgehend abgeschlossen ist:

> *Der erste Schritt für den digitalen Menschenschutz bedeutet, über hunderte von Jahren erarbeitete demokratische Regeln und daraus abgeleitete Gesetze der vordigitalen Zeit weitgehend in der Digitalisierung beizubehalten.*

Die Digitalisierung bietet für eine demokratische Gesellschaft erhebliche Chancen:

> *Im zweiten Schritt für den Menschenschutz sind die gesellschaftlichen Möglichkeiten gemäß dem Stand der Technik und die bestehenden Gesetze proaktiv zu optimieren.*
>
> *Eine Automatisierung soll für den Menschenschutz Aufgaben erleichtern, ohne dabei die vordigitale Verfügungsgewalt der betroffenen Akteure einzuschränken.*

Für den zweiten Schritt müssen staatliche Anreize geschaffen werden, damit überhaupt eine Start-up Kultur entstehen kann, welche sich mit Menschenschutz beschäftigt. Hierfür wiederum ist wichtig, dass international Patentanmeldungen systematisch in Bezug auf ihre gesellschaftliche Strukturrelevanz ausgewertet werden. Die Patentanmelder selbst sehen möglicherweise nicht das Potential ihrer Idee für den Demokratieerhalt. Eine solche Auswertung könnte von den je Sprachraum für das EU-D-S zu gründenden Genossenschaften vorgenommen werden.

Bei einer proaktiven Gesetzgebung unter Einbeziehung speziell zu gründender neuer Organisationen, wie ich das mit GISAD im Rahmen des EU-D-S vorschlage, bestehen im TAB-Bericht genannte zentrale Probleme nicht: (8.3 S230) „Ein zentrales Problem stellt die Frage der Verantwortungszuschreibung dar: Obschon als Systeme zur Entscheidungsunterstützung ausgelegt, sprechen verschiedene Gründe dafür, dass das Prinzip der menschlichen Letztverantwortung bei automatisierten Beobachtungstechnologien zunehmend untergraben werden könnte. (Kap. 7.2.5). Wenn aber eine individuelle Verantwortungszuschreibung nicht mehr gegeben ist, kann niemand für unrechtmäßige oder unmoralische Handlungen zur Rechenschaft gezogen werden." Wie ich später ausführe, ist zudem die Betrachtung einzelner Beobachtungstechnologien zu kurz gedacht. Nur in einer technologischen Gesamtbetrachtung lassen sich die Demokratie auflösenden Tendenzen eines Konglomerats nichteuropäischer Technologieanbieter erkennen.

In einem dritten Schritt für den Menschenschutz ist zu überprüfen, in wieweit Technologie möglichst nachhaltig, für breite Bevölkerungsgruppen verfügbar und verständlich gestaltet werden kann.

Weiterhin ist zu überprüfen, ob die Technologie im Falle eines Politikwechsels für ein autokratisches System missbraucht werden kann.

Vorhandene Technologien für den Menschenschutz sollten mit einer neuen Priorisierung in ihrer Anwendung und teilweise ihrer Konzeption neu gedacht werden:

- Wurde Technikspärsamkeit berücksichtigt und weitgehend auf Updates verzichtet?
- Sie die Auswirkungen der Technologie für die Bürger verständlich?
- Können die Bürger mit der Technologie interagieren?

In einem vierten Schritt für den Menschenschutz geht es um die konkreten, aktuellen, vordigitalen Einsatzpraktiken, welche durch Beobachtungstechnologien abgebildet werden sollen.

In einem fünften Schritt für den Menschenschutz sind in eine Evaluation alle beteiligten Akteure – auch die Bürger – einzubinden, um mögliche nichtintendierte Wirkungen und Folgen des Technologieeinsatzes in Zukunft auszuschließen.

Die Diskussion über die Angemessenheit eines Mittels erübrigt sich weitgehend, wenn man die Beobachtungsstrukturen vom Bürger her denkt: (7.4.4 S219) „Ist die Geeignetheit und Erforderlichkeit des Einsatzes einer Beobachtungstechnologie zu bejahen, muss dieser schließlich auch angemessen (verhältnismäßig im engeren Sinne) sein, um ein Übermaß an Grundrechtseinschränkungen zu verhindern." Dafür muss sich jedoch der Gesetzgeber auch in der Verantwortung sehen, das Übermaß an Grundrechtseinschränkungen durch eine geeignete digitale Infrastruktur der Daseinsvorsorge zu unterbinden. Wie im Folgenden ausgeführt, erfüllt das EU-D-S Konzept die Verhältnismäßigkeit im engeren Sinne und erhöht bei Einbindung der Bürger in eine soziale Kontrolle sogar die Effekte der Gefahrenabwehr und Strafverfolgung.

3 Übertragung der Täteridentifizierung aus dem vordigitalen Bereich

Es gibt ein Konzept der Täteridentifizierung, welches sich weltweit durchgesetzt hat und bezüglich seiner Effizienz nicht infrage gestellt wird. Gemeint ist das KFZ-Kennzeichen.

Die Polizei hat im ersten Schritt die gleichen Rechte, wie jeder anwesende Bürger. Ein eindeutiges Kennzeichen wird bei einem Vorfall erkannt. In einem zweiten Schritt gibt es ein gesetzlich vorgeschriebenes Verfahren, wie der KFZ-Halter identifiziert werden kann.

Letztendlich ist es eine regionale Identifizierungsstelle, welche über das Länderkennzeichen und das Kennzeichen des Kreises gefunden wird. Diese Institution stellt entsprechend geltender Gesetze Informationen zur Verfügung.

Überträgt man das KFZ-Kennzeichen-Konzept auf die digitale Demokratie, so können weitgehend vorhandene Gesetze aufrechterhalten werden.

Allerdings ist die Erstellung der Kennzeichen aufwendig. Es müssen Stempel ausgestellt und Fahrzeugpapiere bei jedem neuen Auto überprüft werden. Digital sind einfachere Verfahren möglich.

Über das eindeutige Kennzeichen können mit Systemen zum automatisierten Kfz-Kennzeichenabgleich Profile erstellt werden, die bei entsprechender Berechtigung einer bestimmten Person zugeordnet werden können. Entsprechend hat der Gesetzgeber mit § 27b BPolG theoretisch sehr rigide geregelt, was mit den Daten passieren darf. Er muss sich allerdings darauf verlassen, dass die Sicherheitsbehörden die Gesetze befolgen.

> *(3.4, S84) „Der weit überwiegende Teil der im öffentlich zugänglichen Raum installierten Videokameras wird allerdings von anderen Akteuren als der Polizei betrieben“.*

Die Softwareindustrie wird im Sinne des Shareholder Values und der Vergrößerung des Absatzmarktes animiert, Tools zu schaffen, welche auch nichtstaatliche Anwender einsetzen können. Schnell können privat ermittelte Daten ins Internet gestellt oder mit anderen Daten verknüpft werden. Es gibt viele Akteure, wie zum Beispiel Versicherungen, welche ein großes Interesse haben, viele Daten miteinander zu verknüpfen. Es gibt eine große Abhängigkeit der Bürger von einer wechselnden Politik, welche jederzeit Gesetze ändern kann.

Nichtstaatliche Anwender benötigen in der analogen Welt einen triftigen Grund, um einen KFZ-Halter zu ermitteln. Diese Situation gilt es zu erhalten:

- Der Bürger wünscht für sich Sicherheit und gleichzeitig das Respektieren seiner Persönlichkeitsrechte.
- Die Sicherheitsbehörden wünschen sich eine möglichst vollständige Aufklärungsquote von Rechtsverstößen.
- Der Gesetzgeber wünscht sich eine weitgehend eindeutige Regelung im Sinne aller Beteiligten.

Für das Sicherheitsinteresse des Bürgers, wie das Aufklärungsinteresse der Behörde ist die Möglichkeit einer eindeutigen Personalisierung sicherzustellen. Allerdings gibt es keinen Grund, diese personenbezogenen Daten in zentralen Datenbanken zu speichern. Das KFZ-Kennzeichen-Konzept hat sich eben über so viele Jahre bewährt, weil die personenbezogenen Daten dezentral gespeichert wurden und so Missbrauch weitgehend ausgeschlossen war.

Wenn vom Gesetzgeber über das EU-D-S Konzept sichergestellt werden kann, dass Profile nicht ohne einen für den Ausnahmefall gesetzlich definierten Anlass Personen zugeordnet werden können, wäre es im Interesse des Bürgers und im Interesse einer nahezu lückenlosen Aufklärung von Delikten, wenn möglichst viele allgemein verwendbare Verhaltensdaten erstellt werden. Alleine durch die Anzahl der über eine Person erstellten Profildaten ist eine Personalisierung durch das finden gemeinsamer Merkmale in derzeitigen Konzepten jedoch möglich!

Wenn jeder Bürger nicht nur eine, sondern 1.000 IP Adressen verwendet, welche ständig auch noch wechseln, wird eine Profilbildung erheblich erschwert, siehe hierzu meine Stellungnahmen zum EU-D-S und meine Patentanmeldungen https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=4&ND=3&adjacent=true&locale=en_EP&FT=D&date=20181213&CC=DE&NR=102017005550A1&KC=A1 und https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=3&ND=3&adjacent=true&locale=en_EP&FT=D&date=20181220&CC=DE&NR=102017005806A1&KC=A1# .

Bürger müssen sich vor unberechtigter Überwachungen durch den Staat oder die Wirtschaft sicher fühlen. Das wird erreicht, indem sie aktiv in den Beobachtungsprozess eingebunden werden. So verlieren sie ihre Bedenken gegen das System. Aus der Überwachung wird eine der vordigitalen Situation entsprechende soziale Kontrolle.

Weiterhin sollte nicht der Staat, sondern von Berufs wegen zu einem bestimmten Verhalten verpflichtete Personen, wie zum Beispiel Anwälte oder Notare, die Zuordnung von personalisierten Daten vornehmen. Personenbezogene Daten, welche dezentral gespeichert und nicht über das Internet abrufbar sind, können nicht bei einem politischen Wechsel missbraucht werden, um die Demokratie auszuhebeln.

Immerhin ist die USA bei den Midterm-Wahlen 2022 knapp an dem Wandel zu einem autokratischen System vorbeigekommen. Der weltweite Rechtsruck kann nur durch die Einführung von Demokratie erhaltenden digitalen Systemen aufgehalten werden.

Das hier vorgestellte Konzept erfüllt die Forderungen des TAB-Berichts: (8.3 S232) „Nicht zuletzt könnten vertrauensbildende und transparenzfördernde Maßnahmen zu einer »Demystifizierung« (Knobloch 2018, S. 40) staatlicher Beobachtungspraktiken beitragen.“

Bei Einsatz des im EU-D-S vorgesehenen ganzheitlichen digitalen Systems, indem gerade die von der Gesellschaft ausgeschlossenen Menschen jederzeit stigmatisierungsfrei an der sozialen Kontrolle teilhaben können und sich in weiteren Schritten sogar für den Berufseinstieg qualifizieren können, teile ich jedoch die Einschränkung des TAB-Berichts nicht: (8.3 S232) „Lässt sich dadurch wohl niemals Übereinstimmung bei allen gesellschaftlichen Gruppen herstellen, so sind Verständnis und Transparenz über die Funktionsweisen, das Ausmaß sowie die Wirkungen und Folgen technisierter Beobachtung notwendige und bedeutende Voraussetzungen für eine informierte gesellschaftliche Verständigung über einen zielführenden und zugleich gesellschaftlich akzeptablen Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit.“ Viele Menschen interessiert eben zuerst ihr Vorteil einer Maßnahme und der muss aus Bürgersicht klar belegbar sein. So ist mir nicht bekannt, dass es spezielle Bevölkerungsgruppen gäbe, welche die KFZ-Kennzeichen grundsätzlich ablehnen würden. Auch hier ist dem Bürger nicht genau bekannt, wie die Halterermittlung funktioniert. Spätestens nach einem unverschuldeten Unfall ist jeder Bürger froh, wenn der Verursacher identifiziert werden kann.

4 Gesamtwirtschaftliche Kostenrechnung

Deutschland befindet sich im demografischen Wandel. Personal wird bei den Sicherheitsbehörden knapp. Auf der anderen Seite entstehen immer mehr frei zugängliche Daten insbesondere durch den Social Media Bereich. Das automatische Erkennen menschlichen Verhaltens durch Algorithmen ist heute noch mehr ein Wunschdenken, als Realität. Wenn überhaupt, sind wiederum hoch komplexe Systeme erforderlich, wie sie nur die Global Player bauen können.

> *(4.2, S121) „Für den einzelnen Sachbearbeiter ist es praktisch unmöglich, mehr als nur eine kleine Auswahl an Inhalten manuell zu erfassen und auszuwerten, um hierauf aufbauend strategische und taktische Entscheidungen abzuleiten. Abhilfe versprechen hier unterstützende Softwarelösungen im Rahmen der Social Media Intelligence (SOCMINT), mittels derer sich die Daten (teil)automatisiert erfassen, klassifizieren, visualisieren und – je nach Funktionsumfang – auch analysieren lassen….“*

> *„Ein Vorreiter in diesem Feld ist die Hessische Landespolizei, die seit 2017 eine angepasste, unter dem Namen Hessendata firmierende Variante der Gotham-Software des US-amerikanischen Herstellers Palantir testet. Die Software soll es ermöglichen, strukturierte wie unstrukturierte Daten verschiedenster Formate und Quellen zu verknüpfen, wobei sich neben Informationen aus verschiedenen polizeilichen Datenbanken auch Daten aus sozialen Medien (etwa die Facebook-Profile von Verdächtigen) einspeisen lassen sollen (letzteres würde jedoch ein Rechtshilfeersuchen an die US-Behörden voraussetzen; Brühl 2018)“.*

Interessant ist diese hessische Vorreiterfunktion vor dem Hintergrund der in meinem Vorwort genannten, 1970 vom hessische Ministerpräsident Albert Osswald geäußerten Überzeugung, Überwachung nie zulassen zu wollen!

Die von mir angedachte Alternative zur umfassenden digitalen Überwachung besteht darin, in einer Art sozialer Kontrolle möglichst viele Menschen in eine WAN anonyme Beobachtung zu integrieren.

Daten sind die Währung der Zukunft. Zum Beispiel ist der Vergleich von Krankheitsbildern sehr wichtig, um Heilmethoden zu finden. Eine wesentliche ökonomische Innovation der Digitalisierung besteht darin, dass die Daten nicht nur einen volkswirtschaftlichen Wert, sondern auch einen hohen Wert für die gesellschaftliche Strukturrelevanz besitzen. Die Staaten verspielen ihre Zukunft gleich mehrfach, wenn sie keine eigene demokratische digitale Infrastruktur zur Verfügung stellen, in der Bürgerdaten mit garantierter Rechtstaatlichkeit generiert, veredelt und verwertet werden.

- Will der Staat sicherstellen, den optimalen gesamtgesellschaftlichen Profit aus den Daten zu generieren, muss er hierfür eine eigene technische Infrastruktur in seiner Hoheit garantieren.
- Um den Erhalt der Souveränität von Staaten und deren Bürger zu garantieren, sollten möglichst viele Daten online zur Verfügung stehen, aber mittels WAN Anonymität persönliche Daten getrennt vom WAN gespeichert sein.
- Eine optimal werthaltige Datenveredelung erfolgt in einem demokratischen Prozess, in dem immer mehrere Personen bei Entscheidungen eingebunden sind.
- Sind die veredelten Daten die Währung der Zukunft, so sollten diese Daten auch nur innerhalb des Staates oder der Staatengemeinschaft frei verwertet werden dürfen.

Es ist fragwürdig, zudem noch nicht ausgereifte Systeme von Anbietern einzusetzen, welche sich nicht explizit dem Erhalt demokratischer Werte verpflichtet haben. Es ist eben wichtig, zu verstehen, dass die Abhängigkeit von Global Playern nicht zum Erhalt der Rechtstaatlichkeit führt, schon gar nicht, wenn die hier entwickelten Konzepte kompatibel zu Autokratien sind. Der Entwicklungsvorsprung globaler Unternehmer kann von Start-ups allein nicht mehr eingeholt werden. Das geht nur noch mit einer ganzheitlichen Initiative der Gesellschaft. Staaten bezahlen Überwachungsfirmen dafür, dass diese ein Know-how entwickeln, um Staaten von sich abhängig zu machen und gleichzeitig die Wertschöpfung der Datenverwertung bei sich zu behalten.

> *Im Sinne eines digitalen Menschenschutzes muss eine gesamtwirtschaftliche Kostenrechnung erstellt werden. Kostenrechnungen von Anbietern, welche den Kaufpreis für eine Software nur über das Verhältnis zur Zeitersparnis des Überwachungspersonals rechtfertigen, dürfen nicht die Grundlage für eine Behördenentscheidung über den Produkteinsatz sein.*

Grundsätzlich ist es fraglich, ob vordigitale demokratische Errungenschaften bei dem reinen Einsatz von Algorithmen ohne ausreichende menschliche Kontrolle jemals erhalten bleiben können. Im Gegensatz zu den USA wird erfreulicherweise derzeit in Deutschland Predictive Policing noch ohne Personenbezug benutzt.

> *(4.3, S 126) „So gewinnen vor allem in den USA personenbezogene Ansätze des Predictive Policing an Bedeutung, um Risikoprofile für einzelne Personen zu erstellen. Neben Vorstrafen und sonstigen polizeilichen Daten werden hier gerade auch Informationen zum sozialen Umfeld von Personen genutzt, die durch die Auswertung sozialer Medien ermittelt werden (Singelnstein 2018, S. 2).“*

Alternativ wäre es in Staaten angebracht, welche die Demokratie erhalten wollen, sich neuen Konzepten zu widmen, in denen die soziale Kontrolle der Menschen mit Algorithmen intelligent verknüpft wird. Meinen Vorschlag zum EU-D-S finden Sie unter https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=1&ND=3&adjacent=true&locale=en_EP&FT=D&date=20190207&CC=DE&NR=102017007331A1&KC=A1# und https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=2&ND=3&adjacent=true&locale=en_EP&FT=D&date=20190124&CC=DE&NR=102017006762A1&KC=A1# .

Geht man weiterhin davon aus, dass viele gesellschaftliche Kosten entstehen, weil Bürger nicht aktiv in die digitale Gesellschaft eingebunden werden, so rechnet sich in einem Gesamtkonzept ein bedingungsgebundenes digitales Bürgergeld. Derzeit entsteht der Eindruck eines ständigen Verteilens von Beruhigungsgeschenken durch die Politik, ohne hierfür von allen eine Gegenleistung zu fordern. Das bedingungsgebundene digitale Bürgergeld sollte eine Aufstockung auf das Bürgergeld ermöglichen, für alle, die an der digitalen Gesellschaft teilhaben und sich durch die Veredelung von Daten etwas dazuverdienen wollen, siehe https://gisad.eu/digital-buergergeld-und-eu-d-s-zwei-die-zusammengehoeren/ . Für den Betrieb und die Verwertung der Daten soll je Sprachraum eine Genossenschaft gegründet werden. Die Genossenschaften schließen untereinander Verträge zur Verwertung der von ihnen entwickelten Software und Hardware. So entsteht ein Datenmarkt, der nicht von Autokratien übernommen werden kann. Die Wertschöpfung kommt unmittelbar in den beteiligten Demokratien an, ohne hierfür protektionistische Maßnahmen ergreifen zu müssen.

Der Natur des Konzeptes entspricht es, dass es richtig umgesetzt, von Autokratien als Gefahr für ihre innere Sicherheit gesehen wird. Wie von mir in einem nicht veröffentlichten Manuskript bereits 2014 bewiesen, hätte der Ukraine-Krieg bei der Einführung eines EU-D-S verhindert werden können. Es scheint mir auch für die Zukunft die einzige Möglichkeit zu sein, um nicht nur die Demokratie, sondern auch die freie Marktwirtschaft zu erhalten.

Es ist ein Schritt in die richtige Richtung, wenn unter 6 und unter 7 des TAB-Berichts gesellschaftliche Auswirkungen technischer Beobachtung behandelt werden. Ich werde mich trotzdem nur in Ausnahmefällen zu diesen Kapiteln äußern, weil sie eben den Einsatz von Technologien hinnehmen, welche bei der Priorisierung vordigitaler Errungenschaften so wegen eines fehlenden Marktes gar nicht entwickelt worden wären. Entsprechend ist auch wahrscheinlich, dass die festgestellten Negativeffekte durch die hier dargestellte Vorgehensweise weitgehend hätten vermieden werden können.

Unsere Priorität muss endlich Konzepten gelten, welche die verfassungsgemäße Ordnung in einer digitalen Gesellschaft erhalten wollen! Demokratien haben sich für die Wirtschaft als nachhaltig verlässlicher Partner bewehrt.

Zu kurz kommt im TAB-Bericht der grundsätzliche Zusammenhang mit der Wirtschaft. Schon immer gab es politische Abhängigkeiten von denen, welche die meisten Steuern zahlen. Doch gerade die deutsche mittelständige Wirtschaft ist nicht der Profiteur der Digitalisierung, auch wenn eine kurzfristige Gewinnsteigerung durch Rationalisierungseffekte das glauben machen wollte. Ob eine Billion Euro reicht, um den Schaden für Europa durch den Ukraine-Krieg zu beziffern, ist fraglich. Der Bundeshaushalt von Deutschland liegt bei nahezu 500 Millionen Euro. Die bekannten Kosten für Cyberangriffen in 2022 liegen laut Bitkom bei 202,7 Milliarden Euro. Man kann von einer erheblichen Dunkelziffer ausgehen. Auch wird Russland seine Cyberangriffe intensivieren.

- Wann ist die Grenze der Kosten erreicht, bei der auch die Unternehmen endlich verstehen, dass jede für die Überwachung eingebaute Hintertür auch gegen Unternehmen und den Staat eingesetzt werden kann?
- Wann hört die Wirtschaft auf, die Verursacher der Strukturprobleme weiter zu fördern, damit diese, unnötig offene Türen unzureichend überwachen?
- Wo sind die Studien, die sich damit beschäftigen, ob Algorithmen, in denen der Mensch nicht als Kontrollinstanz eingebunden wird, mehr schaden, als sie nutzen?
- Die Kosten, um alle Deutschen in ein EU-D-S zu integrieren, schätze ich auf einmalig 2,4 Milliarden Euro. Eine Ersparnis von einem Prozent der Kosten für Cyberangriffe würde ausreichen, um das EU-D-S innerhalb eines Jahres zu refinanzieren! Aufgrund der Möglichkeiten, über das EU-D-S Geld zu verdienen, sind die laufenden Kosten inklusive dem gezahlten bedingungsgebundenen Digital-Bürgergeld nach einer Anlaufphase gedeckt.

5 Soziale Kontrolle statt Überwachung

> *(7, S199) „Der Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit ist immer mit gesellschaftlichen Auswirkungen verbunden. Dazu gehören die intendierten Wirkungen der jeweiligen Beobachtungspraktiken – bei der offenen Videobeobachtung im öffentlich zugänglichen Raum beispielsweise verhaltensbeeinflussende Wirkungen im Hinblick auf eine Abschreckung von potenziellen Straftätern und eine Steigerung des Sicherheitsempfindens der Bürgerinnen und Bürger (Kap. 3.4.4) –, aber auch potenzielle unerwünschte Wirkungen. Im Fokus öffentlicher und politischer Debatten stehen insbesondere mögliche Einschüchterungseffekte im Kontext von breit streuenden Beobachtungstechnologien, deren Einsatz typischerweise eine Vielzahl von Personen betrifft, die selbst keinen Anlass für die Beobachtung gegeben haben.“*

Hier wird die falsche Reihenfolge der Schritte überdeutlich. Die Amerikaner machen es. Wir wollen nicht zurückstehen. Erst einmal ausprobieren und nachher sehen, welche Konsequenzen es hat.

Bereits 1950 hat der amerikanische Soziologe David Riesman visionär die These aufgestellt, wir würden uns von einer innengeleiteten zu einer außengeleiteten Gesellschaft hin entwickeln. Wer die Reize steuert, die auf uns einströmen, steuert auch uns. Es kann bisher nicht erforscht sein, welche gesellschaftlichen Veränderungen zu jetzigen Situation durch die Gestaltung einer aktiven digitalen Demokratie möglich gewesen wären, wenn es diese Entwicklung nicht gibt. Man kann nur das Heute mit der vordigitalen Zeit vergleichen. Die aktuelle Entwicklung der USA mit einer tiefen Spaltung zwischen zwei politischen Lagern ist das Ergebnis einer unreflektierten Digitalisierung. Vielzulange haben wir den Blick auf die amerikanischen Technologien gerichtet, obwohl unsere eigene demokratische Entwicklung bisher gesünder verlaufen ist. Es wurde eben bis heute nicht berücksichtigt, wie sehr digitale Plattformen unser tägliches Leben beeinflussen und verändern. Meinst gibt es enge Synergien zwischen globalen Social Media Plattformen, Suchmaschinen und der Überwachungsindustrie.

Der Blick auf die vordigitale Situation hilft immer. Niemand würde von einer Überwachung ausgehen, wenn er in der überfüllten Innenstadt von vielen Menschen gesehen wird. Selbst wenn man gelegentlich einen Nachbarn grüßt, wird das nicht als Überwachung empfunden. Auf der anderen Seite funktioniert die soziale Kontrolle. Wer nackt durch eine Menschenmenge geht, muss sich Blicken aussetzen. Möglicherweise wird darüber von anderen Menschen geredet. Auch kann es vorkommen, dass das Verhalten der Polizei gemeldet wird. Im Ergebnis kommt es sehr selten vor, dass jemand selbst bei heißem Wetter nackt durch die Straße geht, obwohl es bei einer Verwarnung oder einem kleinen Bußgeld bleiben wird, solange die Nacktheit nicht mit einer sexuellen Handlung verbunden ist.

Genau diese vordigitale Situation gilt es digital abzubilden. Damit soziale Kontrolle nicht zur Überwachung wird, habe ich folgende Voraussetzungen definiert:

Alle Bürger müssen eine vergleichbare technische Möglichkeit der Beobachtung wie die Sicherheitsbehörden erhalten.

Die digitale Begegnung zwischen sozialem Beobachter und Kontrolliertem muss zufällig sein. Optimal sind mehrere Beobachter eingebunden.

Es muss eine einfache Möglichkeit geben, eine Beobachtung zu melden. Die Priorität, in der Beobachtungen von Sicherheitsbehörden zur Kenntnis genommen werden, sollte nicht nur vom gemeldeten Tatbestand, sondern auch der Anzahl der gleichartigen Meldung von mehreren Beobachtern abhängig gemacht werden.

6 Einsatz der sozialen Kontrolle in den einzelnen Anwendungsfeldern

Die Aufteilung der Kapitel 3,4 und 5 des TAB-Berichts halte ich für hochproblematisch. Eine Technik geprägte Arbeitsweise wird zementiert. Oft sind es ausländische Technologieentwickler, welche nur im beschränkten rechtlichen Zugriff der Staaten sind, welche den Einsatz von Überwachungstechnologie forcieren. Es entsteht für Überwachungsakteure eine Abhängigkeit von einzelnen Firmen bezüglich des Kaufs, der Updates und dem Vertrauen auf die rechtskonforme Behandlung von Daten. Im aktuellen Umfeld, in dem Autokratien vor Kriegen nicht zurückschrecken, müssen Technologien unbedingt aus den vordigitalen demokratischen Errungenschaften abgeleitet werden. Die von mir für den Menschenschutz geforderte Reihenfolge des Vorgehens ist einzuhalten.

Entsprechend aufwendig gestaltet es sich, den umfangreichen TAB-Bericht in diese Stellungnahme zu übertragen. Eine endgültige Würdigung des Themas sprengt den Rahmen meiner Möglichkeiten.

Sozialen Kontrolle definiere ich wie folgt:

> *Bisherige als Überwachung bezeichnete Maßnahmen werden im Menschenschutz solange als soziale Kontrolle bezeichnet, wie die Maßnahmen der Sicherheitsbehörden in gleicher Weise von in die Maßnahmen zufällig involvierten Bürgern beobachtet werden können.*
>
> *Gemäß der informationellen Selbstbestimmung muss der sozial Kontrollierte von den Möglichkeiten der Beobachtung Kenntnis haben.*
>
> *Für den Menschenschutz sind Systeme zu schaffen, welche bei jeder Konfrontation mit Überwachungstechnologie im ersten Schritt eine soziale Kontrolle erwarten lassen.*
>
> *Kann von dieser sozialen Kontrolle im Einzelfall nicht ausgegangen werden, so darf eine Überwachung nur durchgeführt werden, wenn der Beobachtete darauf ausdrücklich aufmerksam gemacht wurde.*

Der anlasslose Einsatz von Videotechnologie im öffentlichen Raum hat sich gemäß TAB-Bericht an besonders gefährdeten Orten als erfolgreich erwiesen. Allerdings ist der Personalaufwand so hoch, dass die Überwachungseffekte weitgehend verpuffen. Hier setzen die Argumente der Technologieanbieter an, welche den Arbeitsaufwand durch Automatisierung mittels Algorithmen reduzieren wollen.

In vielen Fälle können alternativ zur Automatisierung digitale Systeme helfen, welche Bürger im Rahmen der sozialen Kontrolle einbinden. Hierdurch wird die Akzeptanz von Überwachungsmaßnahmen erheblich gesteigert. Jedermann kann kontrollieren, was die Sicherheitsbehörden machen. Eine Unterstützung durch Algorithmen ist bei Prozessen der sozialen Kontrolle möglich. Allerdings sollten Algorithmen den Workflow optimieren und den Beobachtern zuarbeiten. Ein erhöhter Personalaufwand der Sicherheitsbehörden kann so mit rechtsstaatlichen Mitteln vermieden werden.

> *Als Ergebnis einer sozialen Kontrolle an die Sicherheitsbehörden weiterzuleitende Informationen dürfen für den Menschenschutz nur über dezentrale, im Interesse des einzelnen Bürgers handelnde Trust-Stationen personalisierbar sein.*

Eine Unterscheidung von polizeilicher und nichtpolizeilicher Gefahrenabwehr ist bisher für den Gesetzgeber wichtig. Im Sinne eines digitalen Gesamtkonzepts gehe ich davon aus, dass alle Akteure miteinander und über die soziale Kontrolle, wo möglich, mit dem Bürger verknüpft werden. Diese Betrachtung des digitalen Menschenschutzes kann heutige Datenschutzbarrieren bei der technischen Umsetzung beseitigen und auch im Sinne der Sicherheitsbehörden wesentlich effektiver sein. Einzuschränken ist anlog zur vordigitalen Situation lediglich das geografische Umfeld der digital sichtbaren Personen.

Zudem sind die politischen Angriffsflächen in Demokratien wesentlich geringer, wenn die staatliche Kontrolle zu Gunsten eines Bürgerengagements reduziert wird.

Das wichtigste Argument für die soziale Kontrolle ist die Akzeptanz von Maßnahmen, welche jeder Bürger nachvollziehen kann. Maßnahmen, welche verstanden werden, bauen Ängste ab. Niemand stört sich in vordigitalen Situationen daran, wenn sein Gesicht zufällig beim Besuch der Innenstadt von vielen Menschen gesehen wird! Die unter 7 (S200) genannten negativen gesellschaftlichen Auswirkungen technischer Beobachtung, wie „das Gefühl des Kontrollverlusts mit dem Ergebnis der Apathie, unterbewusster psychologischer Effekte und das Ergebnis eines vorauseilenden Gehorsams“ können weitgehend reduziert werden, wenn die digitale soziale Kontrolle sich nicht wesentlich von der vordigitalen sozialen Kontrolle unterscheidet. Dafür wiederum ist technisch und normativ sicherzustellen, dass nicht der Einzelne das Konzept aushebeln kann, in dem er die, nicht für die Überwachung gedachte Momentaufnahmen speichert, analysiert oder Dritten zugänglich macht. Hierfür ist noch technische Pionierarbeit zu leisten.

Im Ergebnis muss ein grundlegendes Sicherheitsgefühl beim Bürger erfüllt werden, vergleichbar einer menschengefüllten gut beleuchteten Straße, in der grundsätzlich die Gefahr besteht, in eine dunkle Seitengasse gezogen zu werden. Wenn der Staat die Verantwortung dafür übernimmt, vordigitale Konzepte der sozialen Kontrolle abzubilden, aber nicht selbst der Anbieter von Sicherheit zu sein, stärkt er die Selbstentfaltung der Bürger, verhindert „negative Chillingeffekte“ (7.1.4, S207) und „eine übertriebene Technikgläubigkeit“ (7.2, S208).

6.1 Nichtpersonengebundene Überwachungstechnologien

Die meisten Überwachungstechnologien können auch nichtpersonengebunden eingesetzt werden. Grundsätzlich sollte angestrebt werden, dass jegliche Beobachtung im Einzelfall und nach richterlicher Verfügung personalisiert werden kann. Das geht bei WAN Anonymität besser als bei einem KFZ-Kennzeichen. Entsprechend ist von einer hohen gesellschaftlichen Akzeptanz und geringen negativen Auswirkungen bei einem EU-D-S auszugehen.

Es stellt sich also die Frage, welche Technologien überhaupt bei welcher Einsatzart der Kategorie der nichtpersonengebundenen Überwachungstechnologien zuzuordnen sind.

Eine Speicherung von Daten im Menschenschutz stellt schon dann einen Personenbezug her, wenn eindeutige personenspezifische Merkmale gespeichert werden.

Wenn die Speicherung mit Ortsangaben verbunden und an einem Ort nur eine bestimmte Gruppe von Menschen zugangsberechtigt ist oder nachweislich exklusiv einen Ort aufsucht, müssen angemessene erweiterte Maßnahmen unternommen werden, um die eindeutige Personenzuordnung zu verhindern.

Andererseits dürfen die Ansprüche an Nichtpersonengebundenheit einer Aufhebung der WAN Anonymität im Einzelfall nicht entgegenstehen.

Im Menschenschutz gehören zu den nichtpersonengebundenen Überwachungen alle Maßnahmen, in denen keine menschlich-spezifischen Merkmale erfasst werden.

Diese Voraussetzungen sind zu erfüllen. Hierbei geht es in der Regel um Situationen, in der die Personalisierung über andere vordigitalen Maßnahmen hergestellt wird.

So können zum Beispiel „LKWs mit Röntgenstrahlen“ (S53) auf den Zigarettenschmuggel hin untersucht werden. Bei positivem Überwachungsergebnis wird über das KFZ-Kennzeichen der Inhaber ermittelt.

Mit „Wärmebildkameras“ (S56) können „aus großer Höhe Brandherde und Glutnester identifiziert werden“. Eine Identifizierung von Personen erfolgt in diesem Fall zum Beispiel über ein Melderegister.

Weltraumgestützte bildgebende Beobachtungstechnologien sind nach dem Stand der Technik wohl noch nicht in der Lage, einzelne Personen sicher zu identifizieren. Allerdings können auch hier anhand einer Umriss- oder Bewegungsarterkennung Bewegungsprofile erstellt werden. In diesem Fall sind sie 6.7.1 „Virtuelle Überwachung“ zuzuordnen.

Luftgestützte Systeme können so benutzt werden, dass sie keine menschlich-spezifischen Merkmale erfassen. So kann zum Beispiel anhand einer Bewegung ein Objekt als menschlicher Läufer identifiziert werden. Merkmale, welche einen Menschen von einem anderen unterscheiden, können entweder wegen einer Unschärfe nicht gespeichert werden oder deren Speicherung wird technisch unterdrückt, in dem die für einen Menschen spezifischen Merkmale bei der Speicherung ausgefiltert werden.

Während der TAB-Bericht technisch strukturiert im Kapitel 3 auch die Ortung vermisster Personen enthält, gehört diese Ortung für den Menschenschutz getrennt. Die Kenntnis der vermissten Person ist sogar Voraussetzung für eine Suchmaßnahme. Entsprechend wird dieser Fall unter 6.10 „Fahndung“ aufgenommen.

Technisch kann ein fließender Übergang zur sozialen Kontrolle oder Überwachung entwickelt werden.

Für den Menschenschutz ist der situative Wechsel von einer nichtpersonenbezogenen Überwachung zu einer sozialen Kontrolle oder WAN anonymen Überwachung zu ermöglichen.

So kann zum Beispiel in einem für die Personalisierung zu unscharfen Bewegt-Bild eine Fluchtbewegung erkannt und allen Bürgern auf einem Platz über Broadcast zur Verfügung gestellt werden, ohne dass hierbei einzelne IP-Adressen oder Geräte der Beobachtenden identifiziert werden. In der Nähe der auffälligen Bewegung stehende Beobachter überprüfen die Situation. Möglicherweise rufen gleichzeitig mehrere Passanten mit einem Alarm eine Kameradrohne herbei und sehen dabei die Überwachungsbilder auf dem Smartphone. Auf dem öffentlichen Platz können Menschen auch vordigital das Gesicht anderer Menschen erkennen. Insofern besteht kein Unterschied zur vordigitalen Situation, wenn die Bilder der nahen Drohne dann scharf sind.

Eine wichtige zu entwickelnde technische Innovation wäre, nicht das ganze Gesicht eines Verdächtigen, sondern nur eindeutige Merkmale zentral zu speichern, über welche die zugehörige Trust-Station identifiziert werden kann. In Echtzeit können bei den Trust-Stationen entsprechende reale Bewegbilder situativ, zum Beispiel nach Auslösen eines Alarms, dezentral gespeichert werden.

Tauchen die eindeutigen Merkmale zum Beispiel bei einer weiteren Straftat auf, kann im Einzelfall und nach richterlicher Verfügung die WAN Anonymität aufgehoben werden, indem die Trust-Station einen Abgleich mit den nicht im WAN gespeicherten persönlichen Daten vornimmt. Die Strafverfolgungsbehörde kann bei jedem so erkannten Merkmal automatisch die hierzugehörige Trust-Station identifizieren. Diese wird aufgefordert, die personenbezogenen Daten herauszugeben. Idealerweise ist die Trust-Station vergleichbar mit einem Rechtsanwalt. Sie handelt mit einem Richter aus, ob nur die zu dem einen Bild gehörenden Daten oder weitere über die gleiche Person gespeicherte Informationen herausgegeben werden müssen.

Eine solche Technologie wurde nach meiner Kenntnis noch nicht eingeführt, weil der Gesetzgeber den Bedarf nicht proaktiv definiert hat. Diese Entwicklung ist nach dem Stand der Technik möglich, wie an meinen Patentanmeldungen erwiesen. Die DSGVO zieht sich in der Regel heute aus der Affäre, indem im privaten Bereich (eines Einzelhandelsgeschäfts) Überwachung erlaubt ist, wenn darauf hingewiesen wurde. Erste Ansätze gibt es im Einzelhandel, nur Konturen von Personen zu speichern, aber nicht die realen Videodaten (siehe auch 3.3.3, S78). Letztendlich ist es ein Verstoß gegen die verfassungsgemäße Ordnung, wenn die Gesetzgebung nicht proaktiv durch Hoheit über eine entsprechende digitale Infrastruktur den Schutz der Persönlichkeitsrechte vorantreibt.

6.2 Soziale Kontrolle im öffentlichen Raum

Als öffentlicher Raum wird für den Menschenschutz ein Bereich definiert, in dem sich verschiedene Menschen zufällig begegnen können, ohne hierfür einer bestimmten Gruppe angehören und ohne einer Zugangskontrolle unterliegen zu müssen.

Für den Menschenschutz ist es nicht relevant, ob sich ein Flughafen oder ein Parkhaus in privatem Besitz befindet. Die ständig auch vom Bundesverfassungsgericht geführte Diskussion zum Datenschutz bei der Privatisierung öffentlich genutzter Einrichtungen zeigt die Komplexität des Problems und überfordert den Bürger. Er ist in der Regel nicht informiert oder in der Lage zu verstehen, welche rechtliche Bedeutung es hat, wenn eine Einrichtung, welche er wie früher nutzt, zu einem privaten Besitzer gewechselt hat.

Grundsätzlich sollte überall da, wo es ohne Sicherheitsbedenken möglich ist, die Zuarbeit einer sozialen Kontrolle für die Sicherheitsbehörden vorgesehen werden. Dabei ist die fehlende garantierte Verfügbarkeit von Bürgern zu berücksichtigen. Ein Problem entsteht nicht, wenn die soziale zufällige Kontrolle keine größeren Risiken birgt, als die nur stichpunktartige Möglichkeit der Beobachtung durch unzureichend verfügbares Sicherheitspersonal.

Verbessern kann man die soziale Kontrolle, indem man sicherstellt, dass immer mehrere zufällige Beobachter an besonders gefährdeten Stellen eingebunden sind.

Will man soziale Kontrolle im großen Stil einsetzen, so sind Anreizsysteme zu schaffen, wie das von mir vorgeschlagene bedingungsgebundene Digital-Bürgergeld.

Auch dann, wenn die soziale Kontrolle im öffentlichen Raum keinen garantierten Mehrwert der vollständigen Beobachtung bietet, ist sie einzuführen. Schließlich funktioniert die soziale Kontrolle in der vordigitalen Gesellschaft in den meisten Fällen gut.

WAN Anonymität bietet die einzigartige Möglichkeit, den Bürgern ein Feedback zu ihrer sozialen Kontrolle zu geben. Bei jeder weitergeleiteten Beobachtung teilt das PDS des Bürgers (Persönliches Digitales System, Hardware auf einem USB-Stecker) eine von seinen 1.000 nur bei der Trust-Station personalisierbaren IP-Adressen mit. Eine Personalisierung ist nicht nötig, um auf die entsprechende IP-Adresse des Beobachters ein Feedback zu schicken. Die kann zum Beispiel aus einem jährlichen Report bestehen, in dem festgehalten wird, ob die Meldungen zu einer Anzeige oder Verurteilung geführt haben. Durch das Feedback werden Beobachter bestärkt, weitere Meldungen vorzunehmen. Auf der anderen Seite können Warnmeldungen verschickt werden, wenn jemand sich als Denunziant aufspielt und mehrfach die gemeldeten Beobachtungen falsch waren.

6.2.1 Bildgebende Beobachtungstechnologien

Gemäß der Definition für den Menschenschutz ist der öffentliche Raum wesentlich umfangreicher definiert, als dies derzeit für den Kameraeinsatz rechtlich vorgesehen ist.

Bei dem derzeitigen Einsatz der Technologien sind komplexe rechtliche Vereinbarungen zwischen Polizeibehörden, Verkehrsbetrieben, Deutscher Bahn und Flughafenbetreiber zu schaffen. Nicht nur durch die zentrale Verknüpfung des Datenabgleichs von immer mehr Videodaten, sondern auch durch die undurchschaubare Rechtslage (S94) wird das Fehlverhalten von Sicherheitsmitarbeitern genauso wahrscheinlich, wie die völlige Verunsicherung der Beobachteten, mit den unter 7 des TAB-Berichts beschriebenen negativen Effekten. Hinzu kommen zunehmend Algorithmen, welche im Sinne ihrer Entwickler arbeiten. Im Sinne der Hersteller erhalten die Sicherheitsbehörden nur über die bekannte Funktionsweise der Überwachungstechnologie Informationen. Teile der Datenverarbeitung können im Verborgenen bleiben.

Gerade um die positiven Effekte der sozialen Kontrolle zu ermöglichen, sind die Grenzen zwischen den verschiedenen privaten und öffentlichen Überwachern aufzuheben. Alle bildgebenden Beobachtungstechnologien im öffentlichen Raum sind zu verknüpfen. Die Verknüpfung hat so zu erfolgen, dass sie sowohl von den Bürgern, als auch von den Sicherheitskräften einfach verstanden und in ihrer Wirkung kontrolliert werden kann. Dafür müssen anlassbezog erfasste Bilddaten dezentral bei einer Trust-Station gespeichert werden. Das massenhafte Speichern von Bildrealdaten, dann auch noch von verschiedenen Akteuren, ist auch für kurze Zeiträume grundsätzlich technisch in öffentlichen Räumen zu unterbinden.

6.2.2 Nichtbildgebende Beobachtungstechnologien

Akustische Beobachtungstechnik kann auch für die soziale Kontrolle freigegeben werden. Dabei lassen sich verschiedenste Technologien entwickeln, um dem Menschenschutz zu genügen.

Die polizeilichen Anwendungsfelder (3.2.1.1, S68) werden in der Regel nicht der sozialen Kontrolle zugeordnet werden können.

Nichtpolizeiliche Anwendungsfelder (3.2.1.2, S68) hingehen können für die soziale Kontrolle geöffnet sein. In der Regel werden jedoch Bürger weder über die entsprechenden Ortungsgeräte verfügen, noch sich im entsprechenden Gefahrenbereich aufhalten. Das Gleiche gilt für die meisten Sensoren (3.2.2, S70).

6.3 WAN anonyme Überwachung im öffentlichen Raum

Überwachung im öffentlichen Raum ist in den meisten Fällen einem Alarm der sozialen Kontrolle nachzuschalten. Der rechtliche Rahmen ist so auszugestalten, dass auch automatisch zum Beispiel aufgrund einer hohen Anzahl gleichzeitiger Beobachtungen von Bürgern eine Überwachung durch das Einschalten mehrerer Kameras erfolgen kann.

WAN anonyme Überwachung greift nur durch Auflösung der Anonymität im Einzelfall durch eine Trust-Station in die Persönlichkeitsrechte ein, nachdem ihre Notwendigkeit durch einen Richter bestätigt wurde. Werden von einer Trust-Station alle einer Person zugeordnete 1.000 IP Adressen mitgeteilt, ist auch eine vollständige Überwachung möglich. Nach Abschluss einer Überwachung muss diese dem Überwachten mitgeteilt werden. Durch einen vollständigen Austausch seiner IP-Adressen kann anschließend die WAN Anonymität wiederhergestellt werden.

6.3.1 Bildgebende Überwachungstechnologien

Überwachung wird in der Regel von den Bürgern akzeptiert werden, wenn diese die Notwendigkeit einsehen. Die wenigsten werden erwarten, zum Beispiel über geheimdienstliche Aktivitäten informiert zu werden. Insbesondere Videokameras in öffentlichen Räumen sind sichtbar. Es führt nach Einführung des EU-D-S zu Irritationen, wenn die Beobachter nicht selbst Zugriff auf diese Kameras im Rahmen einer sozialen Kontrolle haben. Es ist zu untersuchen, in wieweit der Überwachungserfolg beeinträchtigt wird, wenn alle jeweils im Sichtfeld eines Betrachters liegenden Kameras von ihm auch bei einer Überwachung eingesehen werden können. Ebenfalls zu untersuchen wäre die Erhöhung der Akzeptanz von Bodycams der Polizisten, wenn die Bilder auch den aufgenommenen Personen zugänglich sind.

Zur Gesichtserkennung habe ich schon ausgeführt, das Methoden entwickelt werden können, in denen ausreichend Merkmale in einer zentralen Datenbank gespeichert werden können, um die Trust-Station zu ermitteln, bei der das zugehörige vollständige Bild gespeichert ist. Sollte ein Foto vorliegen und nach einer Person in vorhandenem Bildmaterial gesucht werden, ist das dem Punkt 6.10 Fahndung zuzuordnen.

KI gestützten Systemen sollten bei identifizierten Auffälligkeiten auch gleichzeitig bei den vor Ort befindlichen Personen und nicht nur den Sicherheitskräften einen Alarm auslösen.

6.3.2 Nichtbildgebende Überwachungstechnologien

Ohne hier auf alle Technologien eingehen zu können, wird die für den Menschenschutz relevante Problematik anhand des Einsatzes von globalen Navigationssatellitensystemen (3.2.3.1, S74) deutlich. So gehören die Bereiche der Überwachung einer Fußfessel, genau wie die Ortung von Personen nach Straftaten von erheblicher Bedeutung in dieser Stellungnahme zum Punkt 6.10 Fahndung.

Anders stellt sich die Situation bei Notrufen dar, in denen die Anrufer sich nicht mehr verständlich machen können. Hier wäre sinnvoll, wenn eine Hilfe der Sicherheitskräfte nicht rechtzeitig kommen kann, die GNSS Koordinaten gegebenenfalls über Broadcast an die umliegenden Smartphones als Hilferuf zu schicken. Dies würde der vordigitalen Situation entsprechen, in dem ein Hilferuf akustisch gehört wird.

6.4 Soziale Kontrolle im nichtöffentlichen Raum

Als nichtöffentlicher Raum wird für den Menschenschutz ein Bereich definiert, in dem Menschen einer Zugangskontrolle unterliegen oder die Erwartung angezeigt wird, den Privatbesitz zu achten.

Die Definition des öffentlichen Raums gibt die Definition des nichtöffentlichen Raums vor. Es ist für die Rechtsprechung notwendig, einen eindeutigen Verantwortlichen zu definieren. Der Menschenschutz geht jedoch immer vom Bürger aus und erwartet die Schaffung eines intuitiv erfassbaren digitalen Rechtsraums.

Geht man von einer konsequent digitalen Gesellschaft aus, so kann das Betreten eines nichtöffentlichen Raums mit einem digitalen Warnton angezeigt werden. Hierbei können gleichzeitig die Regeln des privaten Besitzers mitgeteilt werden.

Es gibt drei Möglichkeiten:

1. Die im öffentlichen Raum vorhandene soziale Kontrolle wird übernommen.
2. Es wird ein privates Regelwerk angezeigt, in dem die Überwachungsmaßnahmen und deren Zusammenführen mit einer sozialen Kontrolle definiert werden.
3. Es wird darauf hingewiesen, dass ausschließlich private Überwachung erfolgt.

Oft bietet vordigital die Gesetzgebung sogar eine Einschränkung der Sicherheit für den privaten Bereich. Aber:

(3.4.3.6 S95) „In welchem Umfang Polizei- und Strafverfolgungsbehörden im Rahmen ihrer Befugnisse (Kap. 3.4.2.4) auf Videomaterial aus privaten Quellen zu Zwecken der Gefahrenabwehr und Strafverfolgung zurückgreifen, ist nicht bekannt.“

Die Überwachung entzieht sich also derzeit weitgehend der Kontrolle durch die Bürger. Hinweisschilder werden meist übersehen und nicht gelesen. Digital lässt sich bei einer Vereinheitlichung der Regeln die Art der Beobachtung übersichtlich zum Beispiel in Form einer Ampel anzeigen.

Soweit im nichtöffentlichen Raum soziale Kontrolle ohne Zugangskontrolle zugelassen wird, ist diese in die soziale Kontrolle des öffentlichen Raums zu integrieren.

Zum Beispiel der Einzelhandel wird es sich gut überlegen, ob er mit zu rigiden Überwachungsmethoden seine Kunden abschreckt. Da das Teilen in der sozialen Kontrolle sowieso auf den visuell sichtbaren Bereich beschränkt ist und die Daten nicht gespeichert werden, ist ein Missbrauch dieser Daten durch Dritte weitgehend auszuschließen. Zusätzlich könnte der Gesetzgeber im Falle der sozialen Kontrolle im nichtöffentlichen Raum unter bestimmten Umständen eine dezentrale Speicherung von Daten zulassen.

Im nichtöffentlichen Bereich ist gegebenenfalls der Bürger selbst entscheidungsbefugt, eigene Daten WAN anonym in Echtzeit zu teilen oder für sich zu behalten. So kann es auf Sportveranstaltungen von Interesse sein, seine Leistungsdaten zu veröffentlichen.

Unterliegt das Betreten eines nichtöffentlichen Bereichs einer Zugangskontrolle, so kann die soziale Kontrolle auf berechtigte Personen eingeschränkt werden.

6.4.1 Bildgebende Beobachtungstechnologien

Ein großes Problem können in einer Gefahrensituation Kameraattrappen darstellen, auf die man sich verlässt. Gerade im nichtöffentlichen Bereich werde diese aufgehängt, um rechtliche Einschränkungen zu umgehen. Im Rahmen des garantierten Einsatzes für die soziale Kontrolle könnten diese Einschränkungen entfallen. Dafür sollten Kameraattrappen nicht mehr erlaubt sein.

Der Zugriff von Sicherheitsbehörden auf Daten aus dem nichtöffentlichen Raum ist durch den Gesetzgeber eingeschränkt. Solange im nichtöffentlichen Raum von einem Benutzer einer sozialen Kontrolle zugestimmt wird, könnte auch Sicherheitsbehörden ein Zugriff auf WAN anonyme Daten erlaubt werden. Dafür sind Maßnahmen zu ergreifen, dass Gesichter grundsätzlich online nicht zusammen mit personenbezogenen Daten angezeigt werden können.

Im Bereich 6.6 „Soziale Kontrolle im virtuellen öffentlichen Raum“ werden die erheblichen Herausforderungen für Maßnahmen gegen digitale Gesichtserkennung weiter beschrieben. Da auch die Selbstdarstellung im Internet ein Persönlichkeitsrecht darstellt, lässt sich die Privatheit nur erhalten, indem in der innerhalb der Hoheit des Staates liegenden EU-D-S Infrastruktur das Veröffentlichen von personenbezogenen Daten jeglicher Art verboten ist. Bilder, welche für die Gesichtserkennung genutzt werden können, gehören dazu. Für die Selbstdarstellung stehen weiterhin die bisherigen Plattformen zur Verfügung. Wie die Interaktion zwischen dem EU-D-S und anderen Plattformen in jedem Einzelfall erfolgt, ist noch nicht konzeptuell zu Ende gedacht und wird der wesentliche Teil im EU-D-S sein, der einer ständigen Anpassung unterliegen wird. Allerdings wird es in der Kommunikation kein Problem sein, personenbezogene Daten eines Kommunikationspartners im eigenen Adressbuch zu speichern. Diese Daten können über das PDS verschlüsselt in der Cloud abgespeichert werden. Insofern werden Personendaten, wenn sie nicht unverschlüsselt über ein Device gesendet werden, nicht als im Internet gespeicherte Personendaten anzusehen, solange der Schlüssel nicht über das Internet erreichbar ist (keine Hintertüren).

Werden zum Beispiel in einem Sportzentrum Bilder dezentral gespeichert, so kann hier Menschenschutz konform eine Identifikation mittels Gesichtserkennung erfolgen, solange die Realbilder nicht Dritten zugänglich gemacht und von diesen gespeichert werden können.

6.4.2 Nichtbildgebende Beobachtungstechnologien

Selbst Sicherheitsscanner für die Personenkontrolle (S58) können im Prinzip der sozialen Kontrolle zugeordnet werden. Solange die Geschlechtsmerkmale kaschiert und nur als gefährlich identifizierte Gegenstände angezeigt werden, ist nichts dagegen einzuwenden, wenn die Scans von allen Personen im Raum gesehen werden können. Es ist der Einsatz von KI hier zu empfehlen, um diskriminierende Bilder wie etwa Prothesen dem Überwacher, aber nicht dem Beobachter anzuzeigen.

6.5 WAN anonyme Überwachung im nichtöffentlichen Raum

Es gibt einen großen Gestaltungsspielraum der Überwachung im nichtöffentlichen Raum. Die menschenschutzkonforme Gestaltung von Zugangskontrollen und Smart Home spielt eine große Rolle.

6.5.1 Bildgebende Überwachungstechnologien

Auch in der vordigitalen Welt gibt es eine definierte Gruppe mit Zugangsrechten. Biometrische Scanner, die Fingerabdrücke oder auch die Iris der Augen erfassen, erhöhen die Sicherheit. Solange die Vergleichsbilder zur Identifikation nur lokal ohne Internetzugriff für den alleinigen Zugriff der Berechtigten gespeichert sind, ist hiergegen aus Sicht des Menschenschutzes nichts einzuwenden.

6.5.2 Nichtbildgebende Überwachungstechnologien

Zunehmend wird mit Smart Home die ganze Regelungstechnik eines Hauses überwacht. Der Grundgedanke von IPv6 ist die Ansteuerbarkeit jedes einzelnen Gerätes über das Internet. Ein solches Konzept bietet erhebliche Sicherheitsrisiken und Möglichkeiten der ungewollten Überwachung durch Dritte. Diese Konzepte werden von Herstellern gepuscht, die über die Wartungsverträge im Zweifel mehr Geld verdienen, als über den Geräteverkauf. Auch erreichen sie so eine hohe Abhängigkeit der Kunden von ihren Produkten. Das Alternativkonzept des EU-D-S setzt soweit möglich, den Menschen als Entscheider weiterhin zwischen die Geräte und den Hersteller. Meldet das Gerät einen Wartungsbedarf, so kann es vom Nutzer mit einem Befehl aus dem nicht mit dem Internet verbundenen Intranet herausgelöst mit dem Internet verbunden werden, siehe https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=7&ND=3&adjacent=true&locale=en_EP&FT=D&date=20170914&CC=DE&NR=102016002956A1&KC=A1# .

6.6 Soziale Kontrolle im virtuellen öffentlichen Raum

Als virtueller öffentlicher Raum wird für den Menschenschutz ein Bereich definiert, in dem sich verschiedene Menschen digital zufällig begegnen können, ohne hierfür einer bestimmten Gruppe angehören zu müssen.

Die Begegnung wird durch digitale Technik unterstützt. Der Austausch von Textnachrichten wird hierunter genauso verstanden, wie das Treffen mit Hilfe eines Avatars.

Der im TAB-Bericht verwendete Begriff des Internets schließt nicht alle möglichen digitalen Interaktionsformen mit ein. Es ist auch im Wesentlichen technisch über das Internetprotokoll definiert. Die für den Menschenschutz getroffene Definition unterscheidet zwischen der Beobachtung der analogen und virtuellen digitalen Welt. Hiermit sollten auch alle zukünftigen Beobachtungsformen berücksichtigt sein. Wenn das EU-D-S von seinem Konzept her möglichst alle Bürger einbindet, um neu virtuell eingestellte Daten zu hochwertigen Informationen zu verdichten, ist der Grundstein zwischen Bürgern und Sicherheitsbehörden für eine von beiden Seiten akzeptierte Interaktion bereits gelegt. Im Ergebnis kann die Polizei auf eine Vielzahl strukturierter Daten zugreifen, ohne die Persönlichkeitsrechte Einzelner verletzen zu müssen. Auch WAN anonym kann (4.1.1 S118) „über entsprechende Beiträge die Feststellung/Identifizierung krimineller Absichten und Personen und die Erforschung und das Verständnis einzelner Phänomenbereiche erfolgen“.

Unter Internetbeobachtung wird verstanden: (4 S117) „

- einfache Methoden wie die Verwendung von Checklisten und Indizes;
- klassische statistische Verfahren wie Regressions- oder Trendanalysen;
- komplexe Anwendungen, die anspruchsvolle Algorithmen und große Datenmengen verlangen;
- maßgeschneiderte Methoden, die bestehende Techniken nutzen, um Daten beispielsweise in Form von Kartendiagrammen zu visualisieren.“

In den meisten Fällen sind für die virtuelle Beobachtung keine persönlichen Daten notwendig. Die Qualität der verfügbaren Informationen wird durch die Bürgerbewertungen erheblich erhöht. Es muss allerdings darauf hingewiesen werden, dass das EU-D-S zusätzlich zu bestehenden Internetplattformen etabliert werden soll. Möglichst alle auf anderen Plattformen öffentlich zu findende Informationen sollen verlinkt werden. Es ist davon auszugehen, dass sich Kriminalität zunehmend ins Darknet verlagern wird, wenn die soziale Kontrolle im virtuellen Raum erheblich erhöht wird. Deshalb werden außerhalb des EU-D-S bisherige Einsatzformen der Internetbeobachtung weiter eingesetzt werden müssen. Ist das EU-D-S etabliert, wird auch Predictive Policing gesellschaftliche Akzeptanz finden, solange es außerhalb des EU-D-S im rechtsfernen Raum eingesetzt wird.

Da die digitalen Beiträge im EU-D-S immer vor mehreren zufälligen Bewertern auf ihren Wahrheitsgehalt hin überprüft werden, wird „die generelle Herausforderung bei der Internetbeobachtung durch die Einschätzung der Qualität der gewonnenen Informationen (4.1.1 S119)“ weitgehend gelöst. Zusätzlich wird die Aktualität von Vorhersagen beim Entstehen kurzfristiger Gefährdungslagen wesentlich erhöht. Wird in einem geografischen oder inhaltlichen Bereich das Ansteigen von Aktivitäten im EU-D-S mit denen im rechtsfernen Internet verglichen, wird die Vorhersagegenauigkeit verbessert.

6.7 WAN anonyme Überwachung im virtuellen öffentlichen Raum

Bedenklich ist es, wenn in einer außengeleiteten, vernetzten Gesellschaft die Polizei Aufgaben übernimmt, welche nach Einführung des EU-D-S durch Bürger im Rahmen einer organisierten virtuellen sozialen Kontrolle übernommen werden könnten. Weder die Gefahrenabwehr, noch die Strafverfolgung gehört in Hände der Bürger. Aber eine Internetbeobachtung als Teil einer vorhersehenden Polizeiarbeit (S 20) bindet viele Fachkräfte, welche an anderer Stelle dringend gebraucht werden. In der Regel sollte zumindest bei einer anlasslosen Beobachtung die soziale Kontrolle immer vorgeschaltet werden. Erst wenn durch die Bürger Anhaltspunkte für ein behördenrelevantes Fehlverhalten beobachtet werden, sollte eine strukturierte Weiterleitung an die entsprechende Überwachungsstelle erfolgen.

(4.2.3 S125) „Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann dann vorliegen, wenn im offenen Internet gewonnene Informationen gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet werden“. Hier ist besonders das Speichern für weitere nicht definierte mögliche Anlässe als kritisch zu sehen. Hingegen ist die soziale Kontrolle im EU-D-S weitgehend transparent. Daten, welche möglicherweise später gar nicht gebraucht werden, werden nicht gespeichert.

6.7.1 Virtuelle Überwachung

Unterstützende Softwarelösungen im Rahmen der Social Media Intelligence (SOCMINT) sind als Überwachung einzustufen. Insbesondere problematisch ist, dass hierbei auch vom Anwender gelöschte Daten weiter berücksichtigt werden können. Im EU-D-S sollten in proaktiver Abstimmung mit der Gesetzgebung eigene Analysesysteme entwickelt werden.

Da im EU-D-S die Anwender über sogenannte Sinnseiten den Zugang zu den Daten finden, müssen sie erst einmal selbst einen Betrag in einem Bereich verfasst haben. Dieser Beitrag wird von verschiedenen zufälligen Bewertern qualifiziert. Außerdem ist WAN Anonymität die Voraussetzung für die Teilnahme am EU-D-S.

Nur wer sich über eine Trust-Station legitimiert und seine IP-Adressen erhalten hat, kann teilnehmen.

Nicht nur für die Sicherheitsbehörden ist im Einzelfall und nach richterlicher Beurteilung die Personalisierung gewährleistet, sondern auch die Bürger untereinander können sich darauf verlassen, nicht mit einem Fake Nutzer zu kommunizieren. Das Gleiche gilt auch für einen verdeckten Ermittler. Dieser muss mit seinen echten persönlichen Daten bei einer Trust-Station registriert sein. So kann Behördenwillkür weitgehend ausgeschlossen werden. Das Provozieren einer Straftat, um die Aufklärungsergebnisse zu verbessern, ist erheblich erschwert und im Zweifel für Bürger nachvollziehbar.

Das eigentliche Problem besteht in den Versäumnissen des Gesetzgebers in den letzten 20 Jahren, den Rahmen für ein digitales demokratisches Gesamtkonzept zu entwickeln. Über Social Media werden mehr Probleme geschaffen, als gelöst. Es ist auch nicht davon auszugehen, dass die digitalen Plattformen hieran etwas ändern wollen. Sie würden damit ihre Geschäftskonzepte gefährden. So bieten zum Beispiel heute Suchmaschinen über die Metatags und wechselnde Werbeanzeigen mehr Werbefläche an, als diese von den Nutzern verarbeitet werden könnten. Elon Musk schaltet Twitter Accounts wieder frei, welche bewusst Unruhe stiften. Künstliche Aufgeregtheiten produzieren Traffic und sind eben nur begrenzt dazu geeignet, echte Gewaltvorbereitung zu erkennen. Entsprechend kritisch ist das Predictive Policing zu sehen, welches mittels Algorithmen versucht, auf Basis eines manipulierten Ausgangsmaterials verlässliche Vorhersagen zu treffen.

„Die rechtliche Einordnung von Verfahren des Predictive Policing ist weitgehend ungelöst“ (4.3.3 S132). Es wird dem Gesetzgeber dingend geraten, seine Ressourcen nicht mit Rücksicht auf wesentlich nichteuropäische Softwareanbieter für dieses Thema zu vergeuden. Mit wesentlich geringerem Entwicklungsaufwand und kalkulierbaren Ergebnissen kann das EU-D-S umgesetzt werden. Funktionieren wird das nach 20 Jahren gesellschaftlicher Fehlentwicklung jedoch nur, wenn die Politik den Willen zu einer digitalen Demokratiebildung mitbringt und es nicht der Privatwirtschaft überlässt, die Risiken zu tragen.

Wird hingegen das EU-D-S allen Bürgern als Infrastruktur zur digitalen Daseinsvorsorge zur Verfügung gestellt, so werden sich mit der Zeit die Mehrheit der seriösen Nutzer vorzugsweise im EU-D-S austauschen. Entsprechend aussagekräftiger werden die Daten-Analysen. Zudem können Massenphänomene zwischen dem EU-D-S und Social Media Programmen in Echtzeit abgeglichen werden. In Kombination werden die Vorhersageergebnisse wesentlich verbessert werden.

6.7.2 Informationstechnische Überwachung

„Informationstechnische Beobachtungstechnologien richten sich auf solche Daten, die eine Person in der berechtigten Erwartung, dass die Informationen vertraulich bleiben, einem informationstechnischen System anvertraut hat“ (5 S133).

Im virtuellen öffentlichen Raum sind die Daten an sich nicht vertraulich. Für den Menschenschutz relevant ist der unbedingte Schutz der personenbezogenen Daten.

An verschiedenen Stellen wird erläutert, wie die personenbezogenen Daten durch getrennte Aufbewahrung vom Internet in einer, einem Rechtsanwaltsbüro vergleichbaren Trust-Station aufbewahrt werden Über das Subnetz lässt sich die Trust-Station identifizieren. Hier muss ohne Internet die Auflösung der IP Adresse zu einer der mit den personenbezogenen Daten gespeicherten je 1.000 IP Adressen hergestellt sind. Siehe hierzu insbesondere 6.9 „WAN anonyme Überwachung im virtuellen nichtöffentlichen Raum“

6.8 Soziale Kontrolle im virtuellen nichtöffentlichen Raum

Als virtueller nichtöffentlicher Raum wird für den Menschenschutz ein Bereich definiert, in dem digitale Zugangsbedingungen erfüllt werden müssen, über welche eine für andere geschossene Gruppe erreicht wird.

Damit ein solches System beim Bürger Akzeptanz findet, ist ein gesellschaftliches Umdenken nötig, in dem der Bürger im Mittelpunkt der Digitalisierung steht. Sicher ist es wichtig, dass Behörden papierlos arbeiten, aber dafür hat sich der Bürger nicht dem Behördenworkflow unterzuordnen. Bei vielen Behördenkontakten ist eine eindeutige Identifizierung durch eIDAS sinnvoll. Nur, wie oft hat der Bürger Kontakt zu einer Behörde? Oft gibt es Jahre keinen Kontakt. So kann eine aus den 1.000 IP Adressen dem eIDAS zugeordnet werden, damit auch hier die Trust-Station eingebunden ist.

Neben der virtuellen Abbildung analoger Ereignisse gibt es unzählige rein virtuelle Räume. Hierzu zählen Chatgruppen genauso wie das Treffen in einer virtuellen Welt mit einem Avatar in einer geschlossenen Gruppe. Durch die Aufteilung aller Daten im EU-D-S in zirka 1000 Kategorien und ein Konzept, bei dem man zu seinem Interesse entsprechende Sinnseiten anlegt, wird eine gewisse Grundqualifikation erwartet, um an einer Gruppe teilnehmen zu können. Die Hintergründe hierzu siehe
https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=12&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120222&CC=ES&NR=2374881T3&KC=T3# und
http://www.getmysense.com/framework-agreement.pdf und
https://www.youtube.com/watch?v=Cbn3D654dxU .

Je nach Qualität einer Sinnseite kann man einen entsprechenden Rank erhalten. Das ist unabhängig davon, wie viele Nutzer die Sinnseite besuchen. Es ist sozusagen das Gegenkonzept zu Social Media, indem ein Influencer die Menschen manipulieren kann, nur weil er lustig oder attraktiv ist.

Zur Teilnahme an einer Chatgruppe wird also mindestens ein kleiner inhaltlicher Beitrag erwartet. Wenn man will, fördert diese Konzept gleichzeitig das lebenslange Lernen, siehe https://gisad.eu/de-eu-initiative-microcredentials-erweiterung-der-lernmoeglichkeiten-zur-foerderung-von-lebenslangem-lernen-und-beschaeftigungsfaehigkeit/ . Dafür kann man sich dann auch mit Gleichgesinnten aus anderen Sprachen sehr einfach vernetzen, was mit der zunehmenden Qualität von eingebundenen Übersetzungsprogrammen erheblich zu einer internationalen Akzeptanz beitragen wird.

Vor allem (4.2, S121) „für die Früherkennung von sicherheitsrelevanten Lagen auf Veranstaltungen“ kann die soziale Kontrolle durch die Anwesenden erheblich helfen. Die Besucher sind WAN anonym unterwegs. Gezielte Falschmeldungen können trotzdem durch einen Ausschluss durch den Veranstalter durch Kontaktaufnahme mit der entsprechenden Trust-Station bestraft werden. Andererseits ist es für einen Besucher mit WAN Anonymität kein Problem, wenn zu seinem digitalen Ticket der Sitzplatz gespeichert ist. Setzt er einen Warnhinweis ab, idealerweise tun das Sitznachbarn auch, so können Sicherheitskräfte sehr schnell reagieren.

6.9 WAN anonyme Überwachung im virtuellen nichtöffentlichen Raum

Eine besondere Stärke spielt das EU-D-S im nichtöffentlichen virtuellen Rau aus. Alle realen Veranstalter haben heute das Problem, in den Sozialen Medien nicht die Fake Accounts herausfiltern zu können. Viele Personen des öffentlichen Lebens trauen sich nicht mehr offen ihre Meinung zu sagen, aus Angst einen unkontrollierbaren Shitstorm auszulösen. Alle diese Phänomene müssen nicht hingenommen werden. Die Politik muss nur ihre Verantwortung begreifen, vordigitale Errungenschaften für die digitale Demokratie zu optimieren. Bürger möchten nicht überwacht werden. Jedoch für ihre Sicherheit finden sie es gut, auf Veranstaltungen zu gehen, in denen jeder, der sich nicht benimmt, rechtlich verfolgt werden kann. Genau das bietet WAN Anonymität. Viele Veranstaltungen kosten Geld. Spätestens beim Bezahlen wird die Anonymität bisher aufgehoben. Die Veranstalter verdienen möglicherweise am Weiterverkauf der Daten zu Werbezwecken Geld. Es entsteht die Notwendigkeit, WAN anonym bezahlen zu können. Genau das habe ich 2022 unter dem Namen „Verfahren für anpassungsfähige, ausfallsichere Transaktionen von Wirtschaftsobjekten“ zum Patent angemeldet. In Zusammenarbeit mit dem Bankstandard der Sofortüberweisungen lässt sich das Konzept mit jedem bestehenden Bankkonto umsetzen. Zudem ist das Bezahlen über Smartphones auch bei einem Stromausfall oder Mobilfunkausfall möglich.

Durch WAN Anonymität ließe sich problemlos ein Platzverbot für Krawallmacher durchsetzen. So könnte zu einer bestimmten Kategorie von der Trust-Station für alle 1.000 IP-Adressen einen Marker gesetzt werden, der den Kartenverkauf automatisch verhindert. Hiermit ließen sich gerichtliche Platzverweise für die verordnete Zeit umsetzen, ohne dass durch eine Personalisierung eine zusätzliche Stigmatisierung erfolgt.

6.9.1 Virtuelle Überwachung

Im nichtöffentlichen virtuellen Raum vertrauen die Bürger darauf, vom Veranstalter geschützt zu werden. Dieser muss sicherstellen, dass Unbefugte draußen bleiben. Technisch ist im EU-D-S die virtuelle Überwachung so gestaltet, dass auch für die Mitarbeiter von Sicherheitsbehörden eine Registrierung über eine Trust-Station die Voraussetzung für die Teilnahme am EU-D-S und wenn der Veranstalter das fordert, auch Voraussetzung für die Teilnahme an einer Veranstaltung ist.

Denkbar wäre, spezielle Trust-Stationen für Sicherheitsmitarbeiter einzurichten. Die IP Adressen wären einer staatlichen Aufsicht bekannt. Den Bürgern gegenüber könnten verdeckte Mitarbeiter anonym bleiben. Bei einem Rechtverstoß wiederum könnte der Betroffene auf die Aufhebung der Anonymität bestehen.

So wäre die Tätigkeit von Mitarbeitern von Sicherheitsbehörden einer sozialen Kontrolle unterworfen. Nach Ablauf einer Überwachungsperiode würden die IP Adressen als Überwachungsadressen öffentlich gemacht. Der verdeckte Ermittler würde vorher mit einem neuen IP Nummernsatz verbunden werden. Mit dem Ermittler interagierende Bürger könnten so zum Beispiel im Nachhinein feststellen, ob sie unrechtmäßig zur einer Straftat provoziert wurden.

6.9.2 Informationstechnische Überwachung

„Informationstechnische Überwachung richtet sich auf Informationen, bei denen der Nutzer auf ihre Vertraulichkeit vertraut. Diese Überwachung ist aus Bürgersicht hochproblematisch. Es geht um das Abhören von Inhalten der elektronischen Kommunikation (Telefongespräche, E-Mails, Datenströme zwischen vernetzten Geräten etc.)“ (5 S133).

Informationstechnische Überwachung ist im nichtöffentlichen Raum für den Menschenschutz für solche Systeme zu verbieten, in denen es geeignete Maßnahmen gibt, durch welche die Notwendigkeit einer Überwachung entfällt.

Die wesentliche geeignete Maßnahme im EU-D-S, welche derzeit für die informationstechnische Überwachung nicht zur Verfügung steht, ist die Garantie, die WAN Anonymität im Einzelfall aufheben zu können.

Zwei Aspekte werden im TAB-Bericht genannt, welche eine informationstechnische Überwachung rechtfertigen (5 S133): „

- Cyberkriminalität,
- Planung und Durchführung von Straftaten mittels Kommunikationstechnik“.

An der Cyberkriminalität kann man gut die Versäumnisse des Gesetzgebers bei der Gestaltung eines digitalen Rechtstaats verdeutlichen. Die meisten technischen Sicherheitskonzepte dienen in erster Linie der Erfüllung von privaten Geschäftsinteressen und dem fragwürdigen Wunsch, die Datenhoheit über die mit den entwickelten Produkten produzierten Daten zu behalten. Auch der Fernzugriff auf die Systeme soll jederzeit möglich sein. Es gibt zahlreiche Möglichkeiten im Internet, seine Identität zu verbergen. Durch ein fehlendes die verfassungsmäßige Ordnung umsetzendes Konzept wurden die unsicheren Systeme zugelassen, welche heute für Cyberkriminalität genutzt werden können. Die Entwicklung lässt sich nicht rückgängig machen. Für den Erhalt des Rechtstaats in der digitalen Demokratie reicht es, wenn man das EU-D-S als gut beleuchtete Hauptstraße einführt. Wer sich dann trotzdem in den rechtsfernen dunklen Gassen der Internetplattformen herumtreiben will, tut das auf eigenes Risiko.

Erst nach Einführung des EU-D-S, in dem durch eine PDS-Hardware zusätzlich zu den 1000 IP-Adressen auch noch Schlüssel verwaltet werden, mit deren Hilfe Kommunikation und Dateien verschlüsselt werden, kann endgültig festgestellt werden, ob und welche Maßnahmen noch nötig sind, um Cyberkriminalität einzudämmen. Siehe hierzu https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=4&ND=3&adjacent=true&locale=en_EP&FT=D&date=20181213&CC=DE&NR=102017005550A1&KC=A1# und https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=3&ND=3&adjacent=true&locale=en_EP&FT=D&date=20181220&CC=DE&NR=102017005806A1&KC=A1# .

Da auch diese Schlüssel von der Trust-Station erstellt werden, ist im Einzelfall eine der vordigitalen Hausdurchsuchung vergleichbare Maßnahme möglich. Dies wurde technisch durch ein Konzept der automatischen Backup-Erstellung gelöst. Das Backupsystem kann fest in einer Wohnung verbaut sein. Ohne eine automatische Backupfunktion würde das PDS keine Akzeptanz bei den Bürgern finden. Schließlich gibt es ohne Schlüssel keinen Zugriff auf die Daten. Siehe hierzu https://worldwide.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20200813&CC=DE&NR=102019000928A1&KC=A1# .

Die im EU-D-S verwendete Ende-zu-Ende-Verschlüsselung ist wesentlich sicherer als die derzeit in den Messenger-Diensten verwendete Sicherheit. Es gibt keine Plattform, die einen Generalschüssel besitzt,

oder mit denen Sicherheitsbehörden Hintertüren verhandelt haben. Da die Verschlüsselung auf dem PDS des Bürgers stattfindet und hierfür keine Onlineupdates vorgesehen sind, ist es unmöglich, ohne die Zustimmung jedes einzelnen Bürgers, Hintertüren einzubauen. Außerhalb der Möglichkeit, über die Trust-Station die Anonymität im Einzelfall in der Absprache mit einem Gericht aufzuheben, besteht der Anspruch, alle Möglichkeiten zu unterbinden, auf mit einem PDS verschlüsselte Daten ohne Kenntnis des Urhebers zuzugreifen.

„Starke Verschlüsselungsverfahren, wie der bei vielen OTT-Kommunikationsdiensten angewendete Advanced-Encryption-Standard-(AES-) 256, können bei heutiger Computertechnik – wenn überhaupt – nur unter extremem Zeitaufwand (Monate bis Jahre) und erheblicher Rechenleistung (Cluster von Hochleistungsrechnern) entschlüsselt werden“ (5.2 S145). Im PDS kann jede einzelne Datei mit einem eigenen AES-256 Schlüssel versehen werden.

„Alternativ könnten Anbieter bzw. Hersteller gesetzlich verpflichtet werden, die verwendeten Schlüssel an eine dafür geeignete Stelle (z. B. eine private oder staatliche Schlüsselverwaltung) zu hinterlegen, um sie im Bedarfsfall unter bestimmten Voraussetzungen (z. B. bei einer richterlichen Anordnung) den Sicherheitsbehörden zugänglich zu machen. Dieser Ansatz birgt das Risiko, dass sich Dritte unbefugt Zugriff auf die zentral hinterlegten Schlüssel verschaffen und somit auf einen Schlag in der Lage wären, sämtliche verschlüsselte Kommunikation mitzulesen (Gesellschaft für Informatik 2015).“

Die von mir in meinen Trusted Web 4.0 Büchern vorgestellte Alternative, eine im Auftrag des Schlüsselinhabers arbeitendes Trust-Station einzuschalten, wurde bisher vom Gesetzgeber nicht berücksichtigt, obwohl meine seit 2016 veröffentlichten 3 Fachbücher zum Trusted WEB 4.0 in die Bibliothek des Deutschen Bundestages aufgenommen wurden, siehe https://books.apple.com/us/book/trusted-web-4-0-konzepte-einer-digitalen-gesellschaft/id1137872975 . Hierdurch ist das im TAB-Bericht genannte Risiko ausgeschlossen, weil die Schlüssel nicht bei einer zentralen Stelle, sondern vielen einzelnen Trust-Stationen hinterlegt sind. Zum Beschaffen vieler Schlüssel müsste man physisch bei den einzelnen Trust-Stationen einbrechen, weil die Schlüssel nicht online zur Verfügung gestellt werden! Es entsteht der Verdacht einer politischen Scheindiskussion, welche die Interessen der Überwacher, jedoch nicht der Bürger vertritt. Hier kann ein Verstoß gegen das Grundgesetz Artikel 20, (2) „Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.“ unterstellt werden. Wie soll das Volk über etwas entscheiden, was ihm vorenthalten wird?

Nach Einführung des EU-D-S wird sicher ein Regelungsbedarf auf den Gesetzgeber zukommen. So könnte zum Beispiel der Abruf einer IP-Adresse und Verfolgung des zugeordneten GPS-Signals erlaubt sein, solange WAN Anonymität gewährleistet werden kann.

Den Grund, die Planung und Durchführung von Straftaten mittels Kommunikationstechnik zu verhindern, ist den Effekten und vor allem dem Aufwand entgegenzusetzen. Die Struktur der EU-D-S erhöht die Hürden für Kriminelle, die sich zu einer Straftat verabreden wollen erheblich. So müssen sie zuerst in einer Kategorie eine Sinnseite erstellen oder zumindest eine Bewertung abgeben. Dafür müssen sie die entsprechende Sprache sprechen. Die Situation ist vergleichbar mit einem Gast in einer Kneipe, der zu niemand Blickkontakt hält.

Es können neue Analysetool entwickelt werden, welche innerhalb des inhaltlich strukturierten EU-D-S Verhaltensauffälligkeiten identifizieren. Ebenfalls ist es denkbar, zur Überprüfung eines Verdachts soziale Interaktionen einzubauen. Nach der Erhärtung eines Verdachts im Einzelfall kann über die Trust-Station die IP-Adresse ermittelt werden.

Die (5.1.4 S183) „Implikation für die Anwendung von informationstechnischen Beobachtungsverfahren“ zeigt erhebliche und zunehmende Probleme der Beschaffung von Kommunikationsdaten in einer heterogenen Betreiberstruktur. Hieran ist aus Sicht des Bürgers zudem problematisch, dass viele Akteure mitmischen und im Ergebnis auch private Kommunikation mitlesen können. Anders verhält es sich im EU-D-S. Der Schlüssel befindet sich grundsätzlich auf der Hardware, ist also in der physischen Verfügungsgewalt des einzelnen Nutzers. Es spielt dann keine Rolle, wo in der Cloud er seine Daten ablegt oder über welchen Weg er kommuniziert, wenn die Daten für Dritte nicht zu entschlüsseln sind.

Selbst für die Sicherheitsmitarbeiter wird der Mehrwert von automatisierter Datenauswertung kritisch gesehen: (7.2.6 S214) „Zu problematisieren ist der Einsatz allerdings dann, wenn Beobachtungstechnologien eingespielte und zuverlässig funktionierende Routinen und Prozesse verändern, die Fähigkeiten und das Erfahrungswissen der Sicherheitsakteure verdrängen oder die sozialen, kognitiven und motivationalen Voraussetzungen des menschlichen Sicherheitshandeln (negativ) verändern (Strohschneider 2010, S. 174; Hempel 2016, S. 118).“

Dabei wurde noch nicht berücksichtigt, dass der Staat die seine Existenz rechtfertigende Kontrolle in die Hände von rechtsfernen Technologieanbietern gibt und solange die erfassten Daten unverschlüsselt im Zugriff dieser Technologieanbieter sind, Missbrauch nicht ausschließen kann.

(Verfassungsrecht S26) „Dies führt etwa dazu, dass der Inhalt ein und derselben E-Mail mal stärker, mal schwächer vor staatlichen Zugriffen geschützt wird, je nachdem, ob die E-Mail gerade übertragen wird (hier greift das Fernmeldegeheimnis) oder sich auf dem Endgerät des Empfängers befindet, wo entweder nur das niedrige Schutzniveau des Grundrechts auf informationelle Selbstbestimmung (beim Zugriff im Rahmen einer Beschlagnahme) oder das hohe Schutzniveau des Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (beim Zugriff durch eine Onlinedurchsuchung) besteht. Solche Zuordnungs-und Bewertungsprobleme werfen die grundlegende Frage auf, ob der grundrechtliche Schutz der kommunikativen Privatheit ggf. neu zu konzipieren wäre, indem nach technisch und sozial anschlussfähigeren und normativ überzeugenderen Kriterien für die Sensibilität digitaler Inhalte gesucht wird. Bislang fehlt es hierzu jedoch weitgehend an konzeptionellen Vorarbeiten.“

6.10 Fahndung

Aus Sicht des Menschenschutzes darf eine Fahndung nur in rechtlich sehr begrenzten Fällen erfolgen.

Sieht man sich die vordigitale Situation an, so werden in rechtlich eindeutig beschränkten Fällen Fahndungsfotos öffentlich aufgehängt. Meist werden Sie jedoch nur von Sicherheitskräften einem kleinen Kreis gezeigt. Richtig sieht der TAB-Bericht (S20) „Im Kontext einer Personenfahndung in Echtzeit wird jedoch überwiegend argumentiert, dass eine automatisierte gegenüber der manuellen Sichtung von Videodaten ein ganz anderes Auswertungsinstrument darstelle, das in seiner Eingriffsintensität weit über die konventionelle Videobeobachtung hinausgehen könne. Vor einem polizeilichen Einsatz solcher Systeme wären daher eigenständige Rechtsgrundlagen zu schaffen, die Anlass, Zweck und Grenzen der Anwendung klar regelten.“ Wieder wird das Dilemma der bisherigen Vorgehensweise des Gesetzgebers deutlich. Technologie ist längst eingeführt, bevor der Gesetzgeber sich in einer Regelung versucht. Im Ergebnis entsteht zunehmend ein Regelwerk, welches niemand anwenden kann. Das Ergebnis der Umsetzung ist dann abhängig von der Kompetenz des Anwenders und vergleichbar mit einer nicht geregelten Willkür.

Das Ziel muss hingegen sein, die rechtliche Situation mittels der Digitalisierung zu verbessern. Da sowieso bei der Gesichtserkennung eine manuelle Nachbearbeitung nötig ist, könnte das Fahndungsfoto auf maschinenlesbar eindeutige Merkmale reduziert, in die Suche gegeben werden. Entweder der Sachbearbeiter hat dezentral ein Foto vorliegen, welches er nach einem Übereinstimmungsalarm mit dem entsprechenden Überwachungsfoto abgleichen kann oder in einer zentralen Datenbank wird das Fahndungsfoto zum Zugriff der Trust-Stationen gespeichert. Wird eine Übereinstimmung einer Überwachung mit den maschinenlesbar eindeutigen Merkmalen gefunden, so kann das Fahndungsfoto von der Trust-Station heruntergeladen und verglichen werden. Insofern stände dann eine Trust-Station nicht nur eindeutig auf der Seite des Überwachten, sondern würde in bestimmten Fällen die Funktion einer Clearingstelle zwischen Justiz und Verdächtigem übernehmen.

Auch die eingeschränkte vordigitale Suche durch einen Fahnder kann digital abgebildet werden. Zum Beispiel könnte einer digitalen Gruppe ein Realbild in einem digitalen Container für eine begrenzte Zeit gezeigt werden. Das Kopieren des Bildes würde technisch unterbunden und unter Strafe verboten.

7 Die Verfassungskrise beenden!

2000 hatte ein Konsortium aus weltweit agierenden Unternehmen den Willen, mein heute noch zum Erhalt von Vielfalt und hochwertigem Content sinnvolles Suchmaschinenkonzept umzusetzen. Aus heutiger Sicht hätten wir in Europa digitale Demokratien, vor denen sich jede Autokratie fürchten würde. Es kam anders und es ist müßig, über die Ursachen zu spekulieren.

Fest steht jedoch, dass die Politik nicht nur die proaktive Unterstützung für den Erhalt der verfassungsgemäßen Ordnung in einer digitalen Gesellschaft versäumt hat, sondern bei vielen kleinen Entscheidungen weggeschaut hat, wenn die Digitalisierung Schritt für Schritt eine verfassungsferne Richtung eingeschlagen hat.

Heute bedeutet es zugegebenermaßen eines erheblichen Kraftakts, ein Konzept umzusetzen, welches die Demokratie in der digitalen Gesellschaft sichern kann. Derzeit wird als Alternative ein Krieg von Russland mit der Ukraine in Kauf genommen, der auch uns erreichen kann. Wäre ein, eine Demokratie erhaltendes digitales Konzept umgesetzt worden, dann müssten sich nicht erneut, wie im zweiten Weltkrieg, Soldaten in einem Krieg gegenüberstehen und sterben. Haben wir uns trotz allen technischen Fortschritts gesellschaftlich nicht weiterentwickelt? Autokratien wurden durch die Digitalisierung mit entsprechenden Tools für Überwachung und Manipulation gestärkt. Auch bei uns ist es für sie möglich, unerkannt und ohne Sanktionen fürchten zu müssen, im Digitalen zu agieren und unsere Demokratie auszuhöhlen. Von Sicherheitsbehörden geforderte Hintertüren helfen hierbei. Selbst die USA stehen derzeit am Rande einer Autokratie. Mit einem konsequenten Konzept der sozialen Kontrolle, das möglichst viele Bürger an der Gesellschaft teilhaben lässt, könnten die Autokratien nicht mithalten. Die hier vorgestellte verschlüsselte dezentrale Kommunikation lässt sich in einem globalen Internet nicht verhindern. Das demokratische digitale EU-D-S könnte sich weltweit verbreiten. Zu aggressive Autokraten müssten befürchten, von innen heraus ihrer Macht beraubt zu werden.

Setzt man zunehmend auf weitgehend durch Algorithmen gesteuerte globale Softwareentwicklungen, so wird zwangsweise eine schleichende Entfernung von demokratischen Prinzipien und Annäherung an Autokratien forciert. So werden ohne zügigen Einsatz des EU-D-S noch so engagierte politische Bemühungen zum Erhalt der Demokratie ins Leere laufen. Nach meiner Einschätzung wird es ohne sofortiger Maßnahmen keine 10 Jahre mehr benötigen, bis unsere Gesellschaft sich im Rahmen der Digitalisierung weitgehend an die Autokratien angenähert hat. Diese Entwicklung ist zwangsläufig, solange sich die Konzepte der Überwachung und Herstellung der digitalen Sicherheit nicht grundsätzlich von denen der Autokratien unterscheiden. Diese Unterscheidung wiederum ist nicht im Interesse eines jeden Herstellers, der einen globalen Markt im Auge hat.

Schon heute sind erste Anzeichen für eine Autokratie-Bildung bei uns zu erkennen. Was uns erwartet, wird schlimmer sein, als das, was wir mit Autokratien verbinden. Die heutigen Autokraten bieten wenigstens noch sichtbare Feindbilder, die man bekämpfen kann. Wir hingegen werden in Scheindemokratien mit unsichtbaren Regeln leben. Hinweise gibt die TAB-Studie zu den Auswirkungen permanenter Beobachtung durch den Staat: (7.1.3 S203) „Dies kann unter Umständen ein permanentes diffuses Gefühl der Verunsicherung auslösen, vor allem auch deshalb, weil Nutzer subjektiv kaum einschätzen können, welchen Verdacht sie erregen müssen, um potenziell staatlichen Beobachtungsmaßnahmen ausgesetzt zu werden (Staben 2016, S. 158).“

Es ist ein schon jahrelang sich manifestierender Ausdruck einer Verfassungskrise und Verfassungsferne der Politik, wenn überhaupt die Frage gestellt wird, ob man eine die Verfassung schützende digitale Infrastruktur einführen soll oder nicht. Die Verfassung muss die Grundlage jeglicher deutschen Politik sein und hat ohne Wenn und Aber im Digitalen umgesetzt zu werden!

Unzureichend wurde bisher untersucht, welche Auswirkungen die permanente Internetüberwachung durch staatliche und nichtstaatliche Akteure auf die Entscheidungsfähigkeit der Politiker hat. Staatliche Überwachung ist nur ein spätes Nachrüsten einer privatwirtschaftlichen Überwachung, in der schon lange nichteuropäische Torwächter die meisten Informationen sammeln. Die künstlich geschürte Aufgeregtheit ist der Treibstoff von Social Media Programmen. Das ist ein wesentlicher Grund, warum Elon Musk auf Twitter Verschwörungstheoretiker wieder zulässt. Sie bringen ihm den Traffic und damit Geld. Jeder Politiker muss jederzeit mit einem Shitstorm rechnen. Dieser kann ohne hierfür mit rechtlichen Folgen rechnen zu müssen, von den Torwächtern direkt oder auch indirekt durch die bevorzugte Positionierung von Informationen Dritter ausgelöst werden. Es ist davon auszugehen, dass viele Verhaltensänderungen, welche der TAB-Bericht (7) Bürgern durch staatliche Kontrolle zuschreibt im erhöhten Maße auf Politiker zutreffen, deren Äußerungen jederzeit unqualifiziert kommentiert werden können. Dabei unterliegt staatliche Überwachung zumindest in vordigitalen Demokratien noch einer Sachlichkeit mit klarer Zielsetzung. Während die öffentliche digitale Wahrnehmung der Politiker so gesteuert ist, dass der mögliche Skandalcharakter, aber nicht die sachliche Auseinandersetzung im Vordergrund steht. Dies hat nichts mit einer im Rahmen des Menschenschutzes vorgeschlagenen sozialen Kontrolle zu tun. Hier gibt es mehrere Kontrollinstanzen, in denen immer mehrere zufällig zusammengesetzte Bürger einen Eintrag diskutieren, bevor dieser mit einem entsprechenden Hinweis freigeschaltet wird. Hierdurch würde eine Versachlichung der Darstellung über Politiker erreicht. Wird diese soziale Kontrolle nicht eingeführt, so gewinnen in der Politik zunehmend Populisten die Oberhand, welche optimal mit den künstlichen Aufgeregtheiten der Sozialen Medien harmonieren. Die Scheindemokratie wird im Ergebnis von demjenigen beherrscht, der die meisten Überwachungsdaten besitzt und hieraus eine öffentliche Wahrnehmung in seinem Sinne gestalten kann.

Ich habe an anderer Stelle bewiesen, dass für mich Artikel 20 (4) des Grundgesetzes zum ersten Mal in der Geschichte der Bundesrepublik erfüllt ist: „Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist.“ Nicht nur die Exekutive, sondern auch die Legislative und Judikative hat sich inzwischen weitgehend auf die Situation eingestellt und Methoden entwickelt, im Sinne der Verfassungsfeinde kritische Entscheidungen durch Untätigkeit auszusitzen oder sich nicht für zuständig zu erklären, wenn verfasungsferne Phänomene auftreten, die eigentlich nicht sein dürften.

Doch die Entscheidungsträger der Wirtschaft sind nicht besser. Bis heute wurde davon ausgegangen, dass Softwareprodukte genau wie Autos global verkauft werden können. Unsere Wirtschaft hat erheblich davon profitiert, dass wir Autos nach China verkaufen. Bei digitalen Konzepten ist das etwas völlig Anderes. Es hat grundsätzliche Auswirkungen auf unsere Demokratiefähigkeit, wenn bei uns marktführende digitale Plattformen und Softwarekonzepte zu Autokratien weitgehend kompatibel sind. Unternehmen sollten in der Lage sein, Kosten, Erträge und Risiken realistisch einzuschätzen. Ein außerordentliches Wachstum erreicht man in neuen Märkten. Demokratie erhaltende digitale Produkte können ein großer neuer Markt werden. Nach einer Studie der Bertelsmann-Stiftung (zdfheute 23.02.2022) sind Demokratien weltweit bedroht. Von 137 untersuchten Ländern sind 67 Demokratien, aber 70 Autokratien. Der Demokratie erhaltende Markt ist nicht global, umfasst aber immer noch fast die Hälfte der Staaten weltweit und ist ausbaufähig. Groß genug, um hier mit anfänglich wenig Wettbewerb schnell zu expandieren, wenn der Staat die durch ihn verursachten Risiken entsprechend absichert!

Als meine letzte Möglichkeit, mich für dem Demokratieerhalt einzusetzen, habe ich einen politischen Antrag gegen den Ukraine-Krieg bis zu den Bundesfachausschüssen der FDP durchgebracht. Hierdurch würde unmittelbar eine Positionierung für die verfassungsgemäße, demokratische Ordnung und gegen Autokratien konzeptuell wiederhergestellt.

Der Wille, die Verfassungskrise zu beenden, würde manifestiert und endlich autokratischen Staaten wie Russland mit modernen digitalen Mittel gewaltfrei Paroli geboten! Das Ganze wäre in einem Pilotprojekt in der Ukraine ohne politisches Risiko möglich, weil es für die Deutschen erst nach einer erfolgreichen Umsetzung in der Ukraine Bedeutung gewinnt.

Hierdurch wäre auch die Frage geklärt, wer Deutschland regiert!

GISAD für ein starkes digitales Europa!
Mit Hilfe der EU die vordigitalen
Errungenschaften erhalten!

GISAD