erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Jörg Pohle*

Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung

Ein Alternativvorschlag

Als das Bundesverfassungsgericht (BVerfG) im März 2010 die Vorratsdatenspeicherung für grundsätzlich mit dem Grundgesetz vereinbar, die konkrete Umsetzung im Telekommunikationsgesetz aber für verfassungswidrig und die entsprechenden Vorschriften für nichtig erklärte,[1] *schrieb es dem Gesetzgeber ins Stammbuch, er sei „bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung"*[2] *gezwungen. Alexander Roßnagel hat das als Notwendigkeit zur doppelten Verhältnismäßigkeitsprüfung beschrieben: Neben die Bewertung der Verhältnismäßigkeit des Einsatzes eines Überwachungsinstruments auf der Grundlage seiner Wirkungen müsse eine Prüfung „auf der Basis einer Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten" treten.*[3] *Für diese Gesamtbetrachtung prägte er dann den Terminus* Überwachungs-Gesamtrechnung[4] (ÜGR).

Überwachungs-Gesamtrechnung – Eine kritische Analyse

Der Begriff der Überwachungs-Gesamtrechnung verspricht mehr, als er halten kann. Eine ÜGR ist trotz ihres Namens weder eine *Überwachungs*-Gesamtrechnung noch eine Überwachungs-*Gesamt*rechnung noch eine Überwachungs-Gesamt-*rechnung*.

Meine Analyse wird sich auf einige ausgewählte Ansätze und Kritiken konzentrieren. An erster Stelle stehen dabei die Vorschläge von Roßnagel und seiner Arbeitsgruppe.[5] Der zweite zentrale Vorschlag wurde vom Arbeitskreis Vorratsdaten Österreich (AKVorrat), seit Ende 2016 epicenter.works, 2016 als *HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze* herausgegeben,[6] ein dritter von Tobias Starnecker in seiner Dissertation über Body-Cams und Dashcams 2017 als „modifizierte und konkretisierte Überwachungsgesamtrechnung".[7] Die umfassendste und zugleich wohl fundierteste Kritik an der ÜGR stammt aus der Feder von Felix Bieker, Benjamin Bremert und Thilo Hagendorff.[8]

Überwachungs…

Eine ÜGR geht über eine Analyse der kumulativen Wirkung von Eingriffen[9], „additiver Grundrechtseingriff"[10] genannt, hinaus und erweitert sie auf die gesellschaftliche Dimension staatlicher Überwachungstätigkeit.

Die Gruppe um Roßnagel sowie Starnecker legen ein traditionell liberales Verständnis von Überwachung als *staatlicher Überwachung* zu Zwecken von Gefahrenabwehr und Strafverfolgung zugrunde. In diesem Verständnis ist Überwachung eher negativ konnotiert und wird durchaus häufig in einen Zusammenhang mit Massenüberwachung, Überwachungsstaat oder Polizeistaat gestellt.

Einen anderen und vor allem sehr viel umfassenderen Überwachungsbegriff gibt es in den *Surveillance Studies:*[11] Überwachung bzw. Surveillance ist im Grunde jede Form von Informationsverarbeitung, in der soziale Akteure – Individuen, Gruppen, Organisationen – sich selbst oder ihre Umwelt beobachten und darauf basierend Entscheidungen treffen und handeln.[12] *New surveillance* ist Surveillance unter Verwendung neuer Datenerhebungs- und -verarbeitungstechniken sowie mehr und neuen Arten von Daten, die verarbeitet und genutzt werden.[13] Dieser breite Überwachungsbegriff, der in den Surveillance Studies rein beschreibend und gerade nicht wertend gemeint ist,[14] wird inzwischen weit über die Surveillance Studies hinaus genutzt – etwa für „Surveillance Capitalism"[15] –, hat dabei aber zugleich die stark negative Konnotation vom traditionellen liberalen, rein auf den Staat bezogenen Überwachungsbegriff geerbt. Und genau diesen Begriff nutzen nun die beiden anderen Arbeiten, die vom AKVorrat und die von Bieker et al., um ihren Untersuchungsgegenstand jeweils einzuführen. Dabei fallen zwei Dinge auf, die alles andere als unproblematisch sind: Erstens wird in beiden Fällen aus terminologischer Koinzidenz auf inhaltliche Identität der Begriffe geschlossen. Zweitens spiegelt sich in der jeweils nachfolgenden Darstellung der konkret zur Analyse herangezogenen Überwachungsmaßnahmen die Breite des eingeführten Überwachungsbegriffs nicht wider.

* *Der Autor bedankt sich bei Michael Plöse für die erkenntnisreiche Diskussion und die erhellenden Kommentare zu diesem Beitrag.*

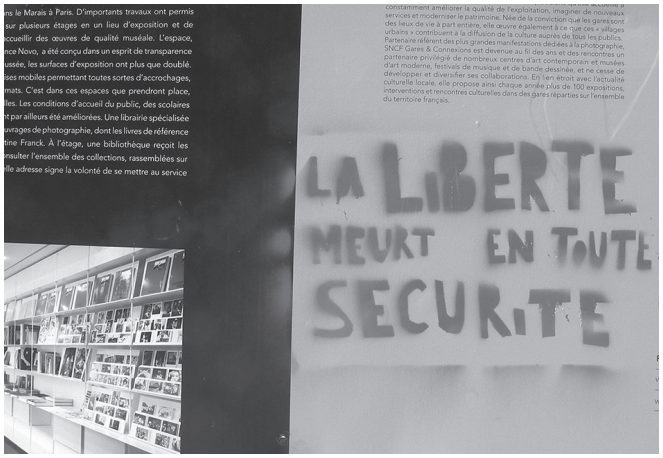
Alle vorliegenden Ansätze beschränken sich auf staatliche Überwachungsmaßnahmen, ob präventiv oder repressiv, ob von Polizeien und Geheimdiensten, vor dem Hintergrund der staatlichen Schutzpflichten für die eigenen BürgerInnen auch gegenüber Behörden anderer Staaten,[16] von der die Debatte um die ÜGR auslösenden Vorratsdatenspeicherung über die Videoüberwachung bis zum Entwurf für eine E-Evidence-Verordnung. Ausgeklammert werden dabei Maßnahmen im Sozial- und Gesundheitsbereich, im Arbeits- und Bildungsbereich oder in der AusländerInnenverwaltung, bei denen es sich um Überwachung im Sinne der Surveillance Studies handelt,[17] soweit nicht Strafverfolgungsbehörden und Geheimdienste auf dort vorhandene Daten zugreifen können. Die private, vor allem die privatwirtschaftliche Überwachung[18] wird nur soweit problematisiert, wie sie Anknüpfungsmöglichkeiten für staatliche Stellen bietet, ob durch Zugriff auf bei Privaten liegende Daten oder auf von diesen betriebene Kommunikationsinfrastrukturen.

… gesamt …

Alle betrachteten Vorschläge problematisieren den Umfang der zu erstellenden Analyse. Eine „Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen", wie es das BVerfG in der Entscheidung über die Vorratsdatenspeicherung forderte, wird teilweise als faktisch unmöglich,[19] teilweise auch als nicht wünschenswert angesehen.[20] Abgesehen von Versuchen einer möglichst umfassenden Darstellung der jeweils existierenden Überwachungsgesetze, -maßnahmen und -systeme Ende der 1970er[21] und Ende der 1980er Jahre[22] scheint es aktuell nur zwei vergleichbar umfassende Sammlungen zu geben – einerseits die Liste der österreichischen Überwachungsgesetze beim AKVorrat, andererseits die Sammlung zur Situation in der Bundesrepublik von Digitalcourage.[23] Moser-Knierim liefert zumindest eine Art Kriterienkatalog für die Auswahl der „Elemente, die den Grad gesamtgesellschaftlicher Überwachung prägen",[24] der allerdings so weit ist, dass es nichts geben kann, was nicht darunter fällt. Hingegen scheinen Roßnagel et al., Starnecker sowie die Bieker et al. davon auszugehen, dass wer immer zur Durchführung einer ÜGR verpflichtet sei, die Liste der Überwachungsgesetze und -maßnahmen selbst zusammenstellen müsse.

Das grundlegende Problem mit der Forderung nach einer tatsächlich gesamthaften Analyse der Überwachung liegt darin, dass sie entweder erstens Unmögliches verlangt, es zweitens keine Obergrenze geben kann, sie drittens zu einer arbiträren Entscheidung über die Inklusion oder Exklusion von gesetzlichen oder tatsächlichen Maßnahmen oder eingesetzten Techniken führt und darum keine sinnvolle Entscheidung erlaubt oder viertens sogar in einem *Whitewashing* endet.

Sie verlangt Unmögliches, wenn es sich um eine Gesamtanalyse der gesellschaftlichen Informationsverarbeitung handeln soll – das ist weit jenseits dessen, was selbst die Wissenschaft derzeit zu leisten in der Lage ist, wie sich unter anderem an den immer noch sehr oberflächlichen Versuchen zeigt, theoretischen Zugriff auf die *digitale Gesellschaft* zu gewinnen. Sie scheitert daran, dass eine echte Obergrenze fehlt: Wenn immer weitere Bereiche der Gesellschaft verdatet werden und zwar in immer höherer – sachlicher, zeitlicher und sozialer – Auflösung, dann verschiebt sich der Maßstab für Vollständigkeit immer weiter nach oben und relativiert dadurch den Umfang der existierenden Überwachung. Sie führt zu einer arbiträren Entscheidung über die Untersuchungsgegenstände, wenn sie zwar Gesamthaftigkeit der Überwachungsanalyse garantiert, sich aber dabei nur hinter der willkürlichen Auswahl des zugrunde gelegten Überwachungsbegriffes versteckt – und sich daran aufgrund der fundamentalen Umstrittenheit[25] von *Überwachung* aber nicht vorbeischmuggeln kann. Und sie wird – das zeigt ein Blick in die Geschichte – in Whitewashing enden: Ruprecht Kamlah hat schon vor vielen Jahren zweimal darauf hingewiesen, dass das BVerfG zwar immer von einem „unantastbaren Kernbereich privater Lebensgestaltung" spricht oder gar einer Intimsphäre als „unverletzlichem Innenraum, der von jedem staatlichen Eingriff freizuhalten ist, in den sich der Bürger vollkommen zurückziehen kann", aber beide seien in der Praxis leer.[26] Bieker et al. stellen richtig fest,[27] dass die Forderung nach einer wirklich umfassenden Analyse nicht zeigen kann, was sie nicht zeigen darf: dass nämlich der Rechtsstaat die Grenze der Rechtsstaatlichkeit überschritten hat.[28]



Freiheit stirbt mit Sicherheit, Foto: privat

… rechnung

Wirklich gerechnet werden soll nach keinem der Vorschläge, und wenn viel über Bewertung gesprochen wird, dann ist das gerade nicht quantitativ gemeint, sondern verweist immer nur darauf, dass der die ÜGR durchführende Akteur etwa eine „wertungsmäßige Betrachtung" vornehmen soll, „um das Bewusstsein für den Umfang der gesellschaftlichen Überwachung zu schärfen."[29]

Moser-Knierim, die auf Roßnagel et al. aufbaut und es erweitert, will in einer ÜGR untersuchen lassen, welche personenbezogenen Daten erstens der Staat „erhebt, erfasst und verarbeitet", zweitens bei Privaten vorhanden sind, auf die der Staat zugreifen kann, und wie drittens sich sowohl die Informations- und Kommunikationstechnik als auch das Nutzungsverhalten darstellt und entwickelt.[30]

Der Vorschlag für das Analyseverfahren vom AKVorrat ist einerseits sehr umfassend und detailliert – fast überdetailliert –, andererseits aber nur in Stichworten ausgearbeitet und an vielen Stellen lückenhaft. Darüber hinaus zielt das Verfahren vorläufig nur darauf ab, einzelne Gesetzesvorhaben zu bewerten

– die Entwicklung eines Verfahrens für eine „vollständige Evaluation im Sinne der ‚Überwachungs-Gesamtrechnung'" wird in die Zukunft verschoben.[31] Den am weitesten ausgearbeiteten Vorschlag liefert Starnecker mit seiner „modifizierten und konkretisierten" ÜGR, die er unter „Zugrundelegung der Erkenntnisse" aus der umweltökonomischen und der volkswirtschaftlichen Gesamtrechnung entwickelt habe,[32] deren starken Fokus auf Quantifizierung er aber nicht übernimmt. Starnecker untergliedert die ÜGR in drei Kategorien:[33]

1. Belastung – die deskriptive Beschreibung der Überwachungsmaßnahmen, systematisiert anhand der Kompetenzträger, Adressaten der Regelung sowie Anlasslosigkeit bzw. Anlassbezogenheit, mit Angaben zur Verwendungshäufigkeit;

2. Maßnahmen – grundrechtsschützende Maßnahmen und Instrumente, wobei er darunter insbesondere prozedurale und technische Schutzmaßnahmen *nach* dem (ersten oder primären) Grundrechtseingriff versteht, also etwa Trennung der Daten oder eine Zugriffskontrolle;

3. Zustand – die Untersuchung des „für den Bürger und die Gesellschaft verbleibende[n] Freiraum[s]" in Form einer „Bewertung und Abwägung aus den vorstehenden Kategorien".[34]

Einbezogen werden soll dabei in die Analyse des Zustands auch die Entwicklung der Technik und ihrer gesellschaftlichen Nutzung – wie viele andere Details ist das von Moser-Knierim übernommen.

Bieker et al.'s Vorschlag, an Stelle der ÜGR eine Gesetzes-Datenschutzfolgenabschätzung nach Art. 35 Abs. 10 DSGVO vorzunehmen, ist einerseits keine Alternative zur ÜGR, sondern stellt eine mögliche Operationalisierung dar, andererseits löst die Gesetzes-DSFA keines der drei von den Autoren am Ende ihres Beitrags genannten Probleme: die Unmöglichkeit, die gesamten Sicherheits- und Überwachungsmaßnahmen zu qualifizieren, die aussagekräftige und vergleichbare Bewertung der jeweiligen Einzelmaßnahmen sowie die Einführung einer „roten Linie".[35] Die Autoren widersprechen sich selbst: Einerseits müsse eine „reproduzierbare Methode zur Ermittlung der Gesamtüberwachung" erst entwickelt werden, damit „von Fall zu Fall vergleichbare Ergebnisse erzielt" würden,[36] andererseits verweisen sie gerade darauf, dass die Gesetzes-DSFA „eine fundierte Basis liefern [würde], um das Ausmaß der Überwachung zu beurteilen".[37]

In allen Vorschlägen bleibt der Bewertungsmaßstab unklar: Woraus ergibt sich bei einer Zusammenstellung aller Überwachungsmaßnahmen, wie groß die individuellen und gesellschaftlichen Freiräume noch bleiben? Zwar wollen sowohl Moser-Knierim als auch Starnecker den noch verbleibenden Freiraum explizit zu einem der Untersuchungsaspekte machen, aber wie? Starnecker verweist etwa darauf, dass „insbesondere auch soziologische Untersuchungen anzustellen" seien.[38] Das ist nur ein Verfahrens-, weder ein inhaltlicher noch ein Bewertungsvorschlag.

Beteiligte Akteure

Fast alle Vorschläge sehen den Gesetzgeber in der Pflicht, eine ÜGR durchzuführen, mit HEAT hingegen richtet sich der AK-Vorrat an die Österreichische Bundesregierung.[39] Roßnagel et al., Moser-Knierim und Starnecker schlagen vor, dass der Gesetzgeber die Bundesdatenschutzbeauftragte mit der eigentlichen Beobachtung und Bewertung der Gesamtüberwachungssituation beauftragen solle, möglicherweise unterstützt durch weitere Forschungs- oder TA-Institutionen. Das ist aus zwei Gründen höchst fragwürdig. Erstens sind Datenschutzaufsichtsbehörden massiv unterausgestattet[40] – eine Situation, die sich nur verschärfen würde, wenn ihnen auch die Aufgabe der Erstellung einer ÜGR übertragen würde. Zweitens ist darüber hinaus stark zu bezweifeln, dass sich an der bisher sowohl von Legislative wie Exekutive gezeigten Ignoranz gegenüber den Analysen, Stellungnahmen und Warnungen der Datenschutzaufsichtsbehörden überhaupt etwas ändern würde.

Ein weiterer Grund spricht dagegen, dem Gesetzgeber die Durchführung einer ÜGR zu überlassen: Abgesehen von einem *Hineinwachsen* in eine umfassende Überwachung durch „technische Veränderungen, veränderte Lebensbedingungen und Lebensweisen oder das Aufweichen der Eingriffsschwellen in der polizeilichen Praxis"[41] wird der Anknüpfungspunkt für die Durchführung einer ÜGR ein je konkretes Gesetzgebungsverfahren sein – gerade vor dem Hintergrund der großen Zahl der Gesetzgebungsverfahren im Überwachungsbereich. Der Gesetzgeber, der dieses Verfahren ja verfolgt, um eine Überwachung auszuweiten, hat darum natürlicherweise ein Interesse, die Gesamtüberwachung *klein zu rechnen* – das jeweils aktuell verhandelte Gesetz wird darum natürlich nie irgendeine *rote Linie* überschreiten. Das macht deutlich, dass die ÜGR eine strukturell dysfunktionale Anreizstruktur hat: Vollständigkeit zu garantieren, ist hart, der Gesetzgeber hat daran kein Interesse, und den Nachteil trägt die Gesellschaft.

Jörg Pohle

Dr. **Jörg Pohle** ist PostDoc am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin, wo er das Forschungsprogramm Daten, Akteure, Infrastrukturen co-leitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Privacy, Surveillance, IT-Sicherheit und Datenschutz und deren Interpretation in verschiedenen Disziplinen und Theorieschulen befasst. Sein Forschungsinteresse gilt dem Schnittbereich von Informatik, Rechts- und Politikwissenschaft sowie Soziologie, dem Feld Informatik und Gesellschaft, der Modellifizierung und ihren gesellschaftlichen Auswirkungen sowie dem Datenschutz durch Technikgestaltung.

Zwei ÜGR-Verbesserungsvorschläge

Der erste Vorschlag betrifft eine Aufteilung der Verantwortung für die Durchführung der ÜGR, die mehr Anreize bietet. Dabei darf sie weder auf schwächere Akteure abgewälzt werden noch auf solche, die sich im Gesetzgebungsverfahren leicht ignorieren lassen. Der Gesetzgeber soll zur Durchführung der ÜGR verpflichtet werden, er darf sie aber nur auf der Basis von Listen von Überwachungsgesetzen und -maßnahmen vornehmen, die von unabhängigen Dritten erstellt werden, etwa Bundes- oder Landesdatenschutzbeauftragten, aber auch der Zivilgesellschaft.[42] Mit der Verantwortung würde auch Macht geteilt und so ließe sich verhindern, dass der Gesetzgeber einzelne Überwachungsmaßnahmen strategisch *übersieht* oder *klein rechnet*.

Der zweite Vorschlag zielt auf ein in der Verfassungsrechtsprechung inzwischen endemisches Problem: Das BVerfG beurteilt bei der Prüfung der Verhältnismäßigkeit von staatlichen (Überwachungs-)Maßnahmen schon seit langem weder Geeignetheit noch Erforderlichkeit.[43] In der Entwicklung des Datenschutzes wurde jedoch gerade dem Kriterium der Erforderlichkeit zentrale Bedeutung beigemessen,[44] bis hin zur Notwendigkeit eines formalen Nachweises:[45] „Eine Information ist zur Erfüllung einer Aufgabe erforderlich, wenn die Aufgabe ohne Kenntnis der Information nicht […] erfüllt werden kann.“[46] Oft sind diese Maßnahmen nicht einmal geeignet, die vom Gesetzgeber avisierten Ziele zu erreichen.[47] Wenn dem Staat nicht eine Beweispflicht für die Geeignetheit und Erforderlichkeit der beabsichtigten oder praktizierten Überwachungsmaßnahmen auferlegt wird, dann wird sich das BVerfG weiter in wolkigen Ergüssen zur Angemessenheit verlieren, die zu letztendlich arbiträren Ergebnissen führen[48] und die Grundrechte strukturell unterminieren.

Freiheitsbestandsanalyse

Das BVerfG hat im Urteil zur Vorratsdatenspeicherung statuiert, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden“ dürfe und dies als zur verfassungsrechtlichen Identität der Bundesrepublik gehörig erklärt.[49] Der Ansatz der Freiheitsbestandsanalyse bildet das konzeptionelle Gegenstück zur ÜGR, indem er *Freiheit* als Startpunkt nimmt und *Überwachung* davon subtrahiert. Er analysiert die Nichterfassung und Nichtregistrierung der Freiheitswahrnehmung selbst – und nur sie.

Freiheit in Raesfeld, Foto: Frank Vincentz, CC BY-SA 3.0

Weil Freiheit ein ebenso fundamental umstrittener Begriff wie Überwachung ist, besteht der erste Schritt in der Operationalisierung von Freiheit. Wird die Verfassungsordnung strukturfunktionalistisch verstanden,[50] ist Freiheit die Menge der Gewährleistungsgehalte[51] der Grundrechte und grundrechtsgleichen Rechte, der deutschen wie der europäischen, sowie der zentralen freiheitsermöglichenden Verfassungsprinzipien wie Rechts- und Sozialstaatlichkeit und Demokratie.

Die Freiheitsbestandsanalyse zieht von den durch die grundrechtlichen Gewährleistungsgehalte sowie die Verfassungsprinzipien aufgespannten Freiheitsräumen jeweils die Überwachungsmaßnahmen ab. Sie ist Aufgabe des Gesetzgebers. Er sollte sie nicht, wie etwa Moser-Knierim vorschlägt,[52] an eine dritte „geeignete Stelle“ übertragen dürfen, da er damit seinen Rechtfertigungszwang in einem Institutionen- und Verfahrensdickicht in nichts auflösen könnte. Dann würde eine Auseinandersetzung um *Verfahrensfragen* die um den *Inhalt* verdrängen, etwa ob das Parlament die von Dritten angefertigte Analyse nur „zur Kenntnis nehmen“ oder „zustimmend zur Kenntnis nehmen“ muss. Der Gesetzgeber würde sich aus der Rechtfertigungspflicht für den in der Analyse abgebildeten Stand der verbleibenden gesellschaftlichen Freiheitsräume stehlen.[53] Ziel muss stattdessen sein, die konkreten rechtlichen Instrumente so auszugestalten, dass der Gesetzgeber gezwungen ist, sich einer *immanent politischen* Auseinandersetzung zu stellen.

Im Ergebnis muss der Gesetzgeber aufzeigen und begründen, welche Grundrechte und welche Freiheiten überhaupt noch und unter welchen Bedingungen überwachungsfrei, d. h. sowohl frei von tatsächlicher als auch von zu erwartender Überwachung, wahrgenommen werden können.

Die Kriterien für die Bewertung der Überwachungsgesetze, -maßnahmen und -praktiken enthalten viele von denen, die in der Diskussion um die ÜGR vorgeschlagen werden – etwa die Frage nach dem Überwachungsorgan, den Adressaten oder die nach Anlasslosigkeit/-bezogenheit, aber auch die Häufigkeit des Einsatzes der Maßnahmen in der Praxis[54] –, gehen aber darüber hinaus. Es gehört dazu, dass die Geeignetheit und Erforderlichkeit der Maßnahmen nicht nur behauptet, sondern tatsächlich nachgewiesen wurden und die Angemessenheit auf dieser Basis geprüft wurde. Weitere empirische Daten aus der Überwachungspraxis und über deren Auswirkungen sind in die Analyse aufzunehmen, wie Daten über Abschreckungseffekte auf das je konkrete Grundrecht und dessen Ausübung und die Identifikation der Hauptbetroffenen(gruppen) der spezifischen Überwachungsmaßnahmen: Es hängt eben nicht nur davon ab, wer als Adressat der Maßnahmen im Gesetzgebungsprozess identifiziert wird, sondern auch, ob in der Praxis vor allem bestimmte Gruppen betroffen sind – Grundrechte dienen nicht ausschließlich und nicht einmal primär dem Schutz einer Mehrheit, sondern im Kern dem Minderheitenschutz.[55]

Sowohl im Hinblick auf einzelne Grundrechte wie auf die verbleibenden Freiheitsräume insgesamt verschiebt die Freiheitsbestandsanalyse die Rechtfertigungslast von den Betroffenen auf den Staat. Für die Betroffenen wird Kritik an der Überwachung vereinfacht, weil sich Behauptungen des Gesetzgebers über die Existenz eines Freiheitsraumes diskursiv vergleichsweise leichter widerlegen lassen. *Ein* Beispiel für eine Überwachungsmaß-

nahme, die diesen Freiheitsraum einschränkt oder gar auflöst, verhindert, dass der Gesetzgeber auf diesen Freiheitsraum verweisen und damit eine echte oder vermeintliche Nicht-Allumfassendheit der Überwachung begründen kann.

Für den Staat wird die Rechtfertigungslast größer: Mit immer mehr Überwachungsmaßnahmen werden die Beispiele von *Räumen* für unüberwachte Freiheitswahrnehmung und deren Beschreibungen tendenziell immer unwahrscheinlicher, wenn nicht gar schlicht abstrus. Damit steigt nicht nur der Rechtfertigungszwang. Die Grenze dessen, was in einer Gesellschaft an Überwachung akzeptabel sein kann, lässt sich sinnvoll operationalisieren: Die Grenze ist erreicht, wenn die vom Gesetzgeber beschriebenen verbleibenden Freiheitsräume für unüberwachtes Wahrnehmen von Grundrechten jenseits der Lebenswirklichkeit der Menschen liegen. Wie immer umstritten Freiheit ist, – gesellschaftliche Zustände, die beschrieben werden als „keine permanente Überwachung der Bewegung von Menschen, die sich in Funklöchern befinden" oder „keine vollständige Überwachung der Kommunikation, wenn selbstkompilierte Messenger genutzt werden" lassen sich nicht mehr als Freiheit verkaufen.

Mit der Freiheitsbestandsanalyse wird damit die Rechtfertigungsordnung im Überwachungsbereich vom Kopf auf die Füße gestellt.

Anmerkungen

1 *BVerfGE 125, 260 – Vorratsdatenspeicherung.*
2 *BVerfGE 125, 260, 324.*
3 *Roßnagel, A. (2010). Die "Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung. In: NJW 18/2010, S. 1238–1242, 1240.*
4 *Roßnagel, A. (2010), 1242.*
5 *Neben dem genannten Roßnagel (2010) vor allem Roßnagel, A.; Moser-Knierim, A. & Schweda, S. (2013). Interessenausgleich im Rahmen der Vorratsdatenspeicherung. Baden-Baden: Nomos, Kapitel 4.4. Beobachtungspflicht und Überwachungsgesamtrechnung.*
6 *Tschohl, C. et al. (2016). HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze. Wien: Arbeitskreis Vorratsdaten Österreich.*
7 *Starnecker, T. (2017). Videoüberwachung zur Risikovorsorge. Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse. Berlin: Duncker & Humblot.*
8 *Bieker, F.; Bremert, B. & Hagendorff, T. (2018). Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf. In: Roßnagel, A.; Friedewald, M. & Hansen, M. (Hrsg.), Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung. Wiesbaden: Springer Vieweg. 139–150.*
9 *Hornung, G. & Schnabel, C. (2010). Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung. In: DVBl., 824–833, 827.*
10 *Starnecker, T. (2017). 365f.*
11 *Lyon, D. (2002). Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. In: Surveillance & Society 1(1), 1–7. Eine recht umfassende Übersicht liefert Marx, G. T. (2015). Surveillance Studies. In: Wright, J. D. (Hrsg.). International Encyclopedia of the Social & Behavioral Sciences.,Amsterdam: Elsevier, 733–741.*
12 *Lyon, D. (1993). The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 3ff.*
13 *Marx, G. T. (2002). What's New About the „New Surveillance"? Classifying for Change and Continuity. In: Surveillance & Society 1(1), 9–29.*
14 *Sewell, G. & Barker, J. R. (2001). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. In: Ethics and Information Technology 3, 181–194.*
15 *Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. In: Journal of Information Technology 30, 75–89.*
16 *Vgl. Bieker et al. (2018), 145.*
17 *Vgl. Ball, K.; Haggerty, K. & Lyon, D. (Hrsg.) (2012). Routledge Handbook of Surveillance Studies. Abingdon: Routledge.*
18 *Vgl. Christl, W. (2017). Corporate Surveillance in Everyday Life – How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. Wien: Cracked Labs – Institute for Critical Digital Culture.*
19 *Bieker et al. (2018), 144ff. im Hinblick auf sowohl die Auswahl als auch die Bewertung der zugrunde zu legenden Überwachungsmaßnahmen.*
20 *Sie könne zu einer „Überforderung des Gesetzgebers", gar zum „Stillstand im Bereich des Sicherheitsrechts" führen, so Starnecker (2017), 371.*
21 *Steinmüller, W. (1979). Der aufhaltsame Aufstieg des Geheimbereichs. In: Kursbuch 56, 169–198; Bölsche, J. (1979). Der Weg in den Überwachungsstaat. Reinbek: Rowohlt.*
22 *Kauß, U. (1989). Der suspendierte Datenschutz bei Polizei und Geheimdiensten. Frankfurt am Main: Campus Verlag.*
23 *https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung.*
24 *Moser-Knierim (2014), 365ff.*
25 *Gallie, W. B. (1956). Essentially Contested Concepts. In: Proceedings of the Aristotelian Society 56, 167–198.*
26 *Zuerst in Kamlah, R. (1970). Datenüberwachung und Bundesverfassungsgericht. In: Die Öffentliche Verwaltung 23(11), 361–364.*
27 *Bieker et al. (2018), 150.*
28 *Es ist darum wenig verwunderlich, dass Roßnagel et al. (2013), 178, diese Grenze erst „nahezu erreicht" sieht. Und selbst Bieker et al. (2018), 150, verweisen am Ende einfach auf das Verhältnismäßigkeitsprinzip und fordern, dass „umso strenger geprüft wird, desto schwerer der Eingriff wiegt."*
29 *Vgl. Moser-Knierim (2014), 237.*
30 *Moser-Knierim (2014), 237ff.*
31 *Tschohl et al. (2016), 11.*
32 *Vgl. Starnecker (2017), 371f.*
33 *Starnecker (2017), 373f.*
34 *Starnecker (2017), 374.*
35 *Bieker et al. (2018), 150.*
36 *Bieker et al. (2018), 145.*
37 *Bieker et al. (2018), 149f.*
38 *Starnecker (2017), 375.*
39 *Tschohl et al. (2016), 26.*
40 *„Defizitbericht" des Hamburgischen Datenschutzbeauftragten (2016), 25. Tätigkeitsbericht Datenschutz 2014/2015. Anhang „Zahlen – Fakten – Defizite – Lösungen".*
41 *Moser-Knierim (2014), 245.*
42 *Wie die Liste von Digitalcourage.*
43 *Hornung & Schnabel (2010), 826.*
44 *Podlech, A. (1973). Datenschutz im Bereich der öffentlichen Verwaltung. Beiheft 1, Datenverarbeitung im Recht (DVR). Berlin: J. Schweitzer Verlag, 54ff.*
45 *Podlech, A. (1982). Individualdatenschutz -- Systemdatenschutz. In: Brückner, K. & Dalichau, G. (Hrsg.), Beiträge zum Sozialrecht – Festgabe für Grüner., Percha: Verlag R. S. Schulz, 451–462, 455f.*
46 *Podlech, A. (1995). Der Informationshaushalt der Krankenkassen: Datenschutzrechtliche Aspekte. Baden-Baden: Nomos, 21.*
47 *Vgl. für den Einsatz von CCTVs zur Senkung der Kriminalität Welsh,*

B. C. & Farrington, D. P. (2002). Crime prevention effects of closed circuit television: a systematic review. UK Home Office Research, Development and Statistics Directorate.

48 Vgl. Kritik bei Schlink, B. (1974). Abwägung im Verfassungsrecht. Berlin: Duncker & Humblot.

49 BVerfGE 125, 260, 324.

50 Vgl. Luhmann, N. (1965). Grundrechte als Institution. Berlin: Duncker & Humblot.

51 Vgl. Rusteberg, B. (2009). Der grundrechtliche Gewährleistungsgehalt: Eine veränderte Perspektive auf die Grundrechtsdogmatik durch eine präzise Schutzbereichsbestimmung. Tübingen: Mohr Siebeck.

52 Moser-Knierim (2014), 244.

53 Zu dieser Pflicht vgl. BVerfGE 113, 273 – Europäischer Haftbefehl.

54 Vgl. Starnecker (2017), 373.

55 Steinmüller, W. (1971). Rechtspolitische Bemerkungen zum geplanten staatlichen Informationssystem. In: Würtenberger, T. (Hrsg.), Rechtsphilosophie und Rechtspraxis. Frankfurt am Main: Vittorio Klostermann, 81–87, 85.

Benjamin Derin

Überwachung, Polizei und ziviler Kontrollverlust

Von der falschen Sicherheit der Präventionsgesellschaft

Staatliche Überwachung und polizeiliche Befugnisse nehmen seit langer Zeit zu, ohne dass ihnen hinreichende Kontrollmöglichkeiten gegenübergestellt werden. Dabei gerät das den Rechtsstaat auszeichnende Verhältnis zwischen Eingriffs- und Abwehrrechten zunehmend aus dem Gleichgewicht. Das Streben nach vermeintlicher Sicherheit wird zur obersten Priorität. Damit einher geht ein sich veränderndes Fremd- und Selbstverständnis der Institution Polizei, die mit immer umfassenderen Aufgaben betraut wird, eine wachsende Rolle im öffentlichen Diskurs einnimmt und sich zugleich der zivilgesellschaftlichen Kritik und Kontrolle zu entziehen droht.

Von Staatstrojanern und Fußfesseln: Wildwuchs der Befugnisse

In den letzten Jahren ist eine massive Ausweitung der polizeilichen Befugnisse vor allem auf zwei sich teilweise überschneidenden Ebenen zu beobachten: zum einen bei der Nutzung technischer Überwachungsmethoden, zum anderen in der landesrechtlichen Gefahrenabwehr in Form der Polizeigesetze.

Neue technische Überwachungsmethoden

Nahezu am Fließband werden derzeit neue heimliche Ermittlungsmaßnahmen geschaffen und bestehende ausgeweitet: Mit der Online-Durchsuchung, Quellen-TKÜ und Telefonüberwachung, *stillen SMS*, *IMSI-Catchern* oder Funkzellenabfragen sowie der erleichterten Datenverwertung einschließlich algorithmengestützter Auswertung hat sich mittlerweile ein massives Arsenal an Überwachungswerkzeugen aufgehäuft. Diese Entwicklung kennzeichnet einerseits ein Zuwachs in der Breite – also neue Maßnahmen und Mittel – sowie andererseits eine zeitliche Vorverlagerung – also die Anwendung weit im Vorfeld konkreter Verdachtsmomente. Ein Ende der Aufrüstung ist nicht in Sicht. Mit der Begründung, der Staat müsse jede technologische Neuerung zur Verbrechensbekämpfung nutzen und drohe, gegenüber den Kriminellen und Terroristen ins Hintertreffen zu geraten (Stichwort *going dark*), hat sich bislang nahezu die gesamte Wunschliste durchsetzen lassen. Auch ohne ausdrückliche rechtliche Grundlage wird eingesetzt, was technisch möglich ist. Es scheint, dass sich Teile der Sicherheits- und Strafverfolgungsbehörden in einer Art Wildem Westen der digitalen Überwachung wähnen. Und angesichts der Verheißungen scheinbar unbegrenzter technischer Möglichkeiten besteht vielerorts offenbar nur ein geringes Bewusstsein für die Risiken, die mit derartigen Methoden einhergehen und für die Auswirkungen, die ihr Einsatz auf die Gesamtgesellschaft hat – von der Gefährdung der allgemeinen IT-Sicherheit durch den unreflektierten Umgang mit Sicherheitslücken und Staatstrojanern bis hin zur Schwächung der demokratischen Zivilgesellschaft durch ein Klima der Überwachung und Repression.

Bundesweite Reformen der Polizeigesetze

Auf dem Vormarsch sind diese modernen Eingriffsgrundlagen sowohl in der Strafprozessordnung (dort zur Strafverfolgung) als auch in den landesrechtlichen Polizeigesetzen (sie regeln komplementär die Abwehr allgemeiner Gefahren außerhalb des Strafrechts). Die seit 2017 anrollende und noch immer nicht abgeschlossene Welle neuer Polizeigesetze, die sich inzwischen auf nahezu alle Bundesländer ausgedehnt hat und zu denen etwa das umstrittene bayerische Polizeiaufgabengesetz gehörte, brachte daneben aber auch eine massive Ausweitung klassischer Befugnisse mit sich. Hierzu gehören je nach Bundesland etwa öffentliche Videoüberwachung, verdachtsunabhängige Kontrollen, Meldeauflagen, Hausarrest, Kontaktverbote, elektronische Fußfesseln, Taser[1] und monatelanger Präventivgewahrsam. Parallel dazu wurde – vor allem mittels des berüchtigten Konzepts der „drohenden Gefahr" – die Schwelle polizeilichen Eingreifens herabgesetzt, sodass die Polizei auf dem Gebiet der Gefahrenabwehr künftig früher Maßnahmen ergreifen darf und dabei weniger Anhaltspunkte dafür darlegen muss, dass die Person, gegen die sich diese Maßnahmen richten, tatsächlich eine Gefahr darstellte (s. Lippa 2018). Althergebrachte Kriterien, nach denen das Handeln der Polizei bislang juristisch beurteilt wurde, verschwimmen zusehends und schaffen immer größere Spielräume für die agierenden Beamten.

Dieser Bereich wirkt im Vergleich zu dem weiter oben beschriebenen High-Tech-Rüstzeug womöglich weniger bedeutsam und