Freiheit für die Technik der Bürgerin und des Bürgers?
- Gedanken zum technologisch geprägten Grundrechtsschutz

Marie-Theres Tinnefeld

Referat am 5. September in der Universität Bremen
Festkolloquium aus Anlass des 60. Geburtstags von
Prof. Dr. Hans-Jörg Kreowski

I. Einführung: Bedenklicher Prozess der Gesetzesbildung

Cato der Ältere, römischer Staatsmann im zweiten Jahrhundert vor Christus, soll jede seiner Reden im Senat mit dem Satz geschlossen haben: *„Ceterum censeo Carthaginem esse delendam“* („Im Übrigen meine ich, dass Karthago zerstört werden muss“). Diese ständige Wiederholung führte nach der Überlieferung dazu, dass der Senat schließlich Cato zustimmte und Carthago im Dritten Punischen Krieg (149-146 v. Chr.) angriff und zerstörte. Die rhetorisch geschickte, nicht immer im Sachzusammenhang motivierte **Wiederholung** war gleichsam der **Brandbeschleuniger** dieser kriegerischen Aktion.

Diese Geschichte aus antiker Zeit ist Ihnen sicherlich bekannt. Vielleicht ahnen Sie auch, warum ich sie meinem Thema voranstelle. Seit den verheerenden Ereignisse von 9/11 sind in den Medien, vor allem im Fernsehen, Terrorakte immer wieder in Endlosschleifen präsentiert worden. Gleichzeitig wurde im „war on terror“ gebetsmühlenartig die Forderung nach mehr Sicherheit in vorher offenen westlichen Ländern wiederholt. Die Kombination vom Endlos-Bild des Terrors mit der ständigen Forderung des Staates nach mehr Sicherheit zu Lasten klassischer Freiheitsrechte hat bislang zahlreiche Antiterrorgesetze produziert. Triumphieren diese Gesetze *„in einer - darf man sagen göttlichen, soll man sagen: teuflischen? - Freiheit“* (Peter von Matt).

Einen solchen Triumph und mithin die schleichende Erosion unseres Rechtssystems hat das Bundesverfassungsgericht häufig verhindern können, indem es Gesetze ganz oder teilweise als verfassungswidrig und für nichtig erklärte. Wesentliche Stichworte sind: der Große Lauschangriff, die Erfassung der Kontostammdaten, die vorbeugende Telekommunikations-Überwachung, das Luftsicherheitsgesetz, die präventive Rasterfahndung, die sogenannte Online-Durchsuchung und schließlich die Einstweilige Anordnung zur sogenannten Vorratsspeicherung. Das umstrittene nationale Gesetz zur Vorratsdatenspeicherung basiert auf einer ebenso umstrittenen EU-Richtlinie, die am Maßstab der Grundrechte zu messen ist.

Schon Wilhelm von Humboldt hat in seiner 1792 fertiggestellten Schrift über „Die Idee zu einem Versuch, die Grenzen der Wirksamkeit des Staates zu

bestimmen“ sinngemäß dargelegt, dass **Sicherheit ohne Freiheit unerträglich** ist. Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Jede Freiheitseinschränkung unter der positiv klingenden Vokabel „Prävention“ könnte sich andernfalls dem negativen Bild eines Überwachungsstaats annähern, in dem anlasslose und vor allem heimliche, technisch gesteuerte Eingriffe für rechtens erklärt werden.

Durch den zunehmenden Einsatz subtiler Informationstechnologien werden neue Gefährdungen grundrechtlich geschützter Freiheiten sichtbar, mit denen sich auch das Forum für Informatiker/innen für Frieden und gesellschaftliche Verantwortung mit seinem Vorsitzenden Hans-Jörg Kreowski in den letzten Jahren nachhaltig befasst hat. Die Abhängigkeit des Grundrechtsschutzes von der Technik ist kaum an anderer Stelle so deutlich formuliert worden wie im Zusammenhang mit der Kritik an der Technik auf diesem Forum. Diese führt letztlich zu der Erkenntnis, dass sich Bürger ohne **Vertrauen in eine sichere Technik** nicht mehr frei und selbstbestimmt in der vernetzten (Welt-) Risikogesellschaft bewegen können (Ulrich Beck).

Das Bundesverfassungsgericht hat sich mit dieser Entwicklung befasst und das grundrechtlich verankerte allgemeine Persönlichkeitsrecht durch neue Schutzdimensionen abgesichert. Nach dem Grundrecht auf Datenschutz hat das Gericht aus dem Persönlichkeitsrecht ein **„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“** (im Folgenden: IT-Grundrecht) abgeleitet, das die freie Entfaltung der Persönlichkeit in Verbindung mit dem Menschenwürdeschutz gewährleistet.

II. Das Bundesverfassungsgericht: Bewahrer lebendiger Grundrechte

Vor mehr als 25 Jahren haben zahlreiche Bundesbürger aus Furcht vor der Undurchschaubarkeit elektronischer Datenverarbeitung, vor dem gläsernen Bürger und vor einer Volksdurchsuchung gegen ein Gesetz zur Volkszählung protestiert. Das Bundesverfassungsgericht hat in seiner Entscheidung zu diesem Gesetz am 15. Dezember 1983 nicht nur auf die Undurchsichtigkeit der technischen Vorgänge bei der personenbezogenen Datenverarbeitung reagiert, sondern es passte auch die Vorgaben des allgemeinen Persönlichkeitsrechts den Bedingungen der automatisierten Datenverarbeitung an und schuf das Grundrecht auf informationelle Selbstbestimmung bzw. auf Datenschutz, worunter auch das rechtlich geschützte Interesse des Einzelnen an Intimität und Privatheit zu verstehen ist. In neueren Entscheidungen spricht das Gericht von einem Grundrecht auf informationelle Privatheit (information privacy). Die Formulierung findet sich bereits bei Alan F. Westin in seinem Werk „Privacy and Freedom“ (1967). Dem Schutz der Privatheit dienen auch spezielle Freiheitsverbürgungen wie das Grundrecht auf Unverletzlichkeit der Wohnung

und das grundrechtlich verankerte Post-, Brief- und Fernmelde- bzw. Telekommunikationsgeheimnis.

Mit seiner ausdrücklichen **Forderung nach Datenvermeidung und Datensparsamkeit** hat das Bundesverfassungsgericht im Volkszählungsurteil eine Allianz von Datenschutz und Technik im Interesse der Privatheit und sicheren Kommunikation angesteuert und gleichzeitig eine zweckfreie Vorratsdatenspeicherung verboten, wie sie z. B. von der Telekom praktiziert wurde und von Sicherheitsbehörden und Geheimdiensten zu präventiven Zwecken gefordert wird.

Die Forderung nach Transparenz der Datenverarbeitung für den Betroffenen ist ein wichtiges Ziel des Datenschutzes. Sie lebt von der Voraussetzung, dass nicht beliebig viele, sondern nur die für einen bestimmten Zweck der Datenverarbeitung und Kommunikation unbedingt erforderlichen persönlichen Daten erfasst werden. Zur Ausgestaltung des Grundrechts auf Datenschutz gehört daher das Prinzip der Datensparsamkeit bzw. sogar das der Datenvermeidung, das in der Nicht-Offenlegung der Identität einer Person besteht, also ihre Anonymität sichern soll.

Dieses **Recht auf Anonymität** ist Teil des Grundrechts auf Datenschutz und somit eine Selbstverständlichkeit im täglichen Leben. Helmut Bäumler hat dies so ausgedrückt: *„Es ist fast so, wie wenn wir atmen, essen und trinken, ohne dass wir überhaupt daran denken, dass wir dabei unser Grundrecht auf Leben realisieren.“* Angesichts der ständigen Beschwörung höchster Gefahren ist dieses Recht jedoch in Misskredit geraten. Wer anonym sein will, macht sich verdächtig; er hat etwas (Gefährliches, Strafbares?) zu verbergen.

Dies vermutet wohl auch der fürsorgliche Präventionsstaat, der bereits im Vorfeld von Straftaten ermitteln und vorbeugende Dateien über Personen erstellen will, von denen er annimmt, dass sie in Zukunft eine Straftat begehen wollen oder werden. Dementsprechend erodieren die Grenzen zwischen Schuldigen und Unschuldigen, und jede Person wird zum Risikofaktor. Bewegen sich die Bürger angesichts dieser Entwicklung *„schlafwandelnd in den Überwachungsstaat?“* - so die berechtigte Frage des auf der britischen Insel lebenden Rechtsinformatikers Burkhard Schäfer.

Die überwiegend von Kommunen betriebenen Kameras zur Videoüberwachung (CCTV-Systeme bzw. Closed Circuit Television) und die größte DNS Datenbank in England weisen in diese Richtung. Sie haben die Zerschlagung von kriminogenen Strukturen schon im Vorfeld eines „Anfangsverdachts“ zum Ziel. Bei genauerem Hinsehen hat sich aber nicht nur die flächendeckende Videoüberwachung in Englands Städten als nutzlos erwiesen. Sie birgt auch große Gefahren für die Rechtssicherheit im Sinne verbürgter Freiheitsrechte des

citizen. Gleichwohl bleibt die öffentliche Zustimmung insbesondere zur CCTV –Überwachung hoch.

Man sollte die technischen Möglichkeiten der Videoüberwachung kennen, wenn man ihr ein vernünftiges, datenschutzgerechtes Maß anlegen will. Hier sei auf geeignete Software (z.B. das Software-Modul „Privacy Protector“ von KiwiSecurity) hingewiesen, mit der man die Videoüberwachung nach den Grundsätzen der Datensparsamkeit und Datenvermeidung effizient gestalten kann.[1]

III. Der Europäische Gerichtshof für Menschenrechte: Schutzschild des Privatlebens

Eine Entwicklungslinie des Datenschutzes wurzelt in der Europäischen Menschenrechtskonvention (EMRK). Art. 8 der Konvention garantiert das Recht auf Achtung des Privatlebens, des Familienlebens, der Wohnung und des Briefverkehrs bzw. der Telekommunikation. Der Artikel gewährleistet mit seinen Teilgarantien einen **weiten Raum der freien Entfaltung der Persönlichkeit**. Er findet sich zusammen mit einer speziellen Datenschutzbestimmung in der EU-Charta der Grundrechte (Art. 7 und Art. 8 EuGRC) wieder, die erst mit der Verabschiedung des Vertrags von Lissabon rechtskräftig wird.

Im Zusammenhang mit der Speicherung von personenbezogenen Daten hat der Europäische Gerichtshof für Menschenrechte im Jahre 2000 den Schutzbereich von Art. 8 wie folgt umschrieben: "*It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings*.“ Auf diese Weise hat das Gericht den Schutzbereich des Privatlebens gegenüber neu auftretenden Gefährdungen nachhaltig erweitert, so dass der Europarechtler Rainer Schweizer Art. 8 als europäisches Auffanggrundrecht bezeichnen kann.

Vor diesem Hintergrund ist zu betonen, dass Zugriffe auf den Informations- und Kommunikationsverkehr etwa bei einem systematischen Abhören aller Telefone in einer Anwaltskanzlei, wie das in der Klage Kopp gegen die Schweiz von 1998 der Fall war, personenbezogene Daten in unzulässiger Weise erheben: Das unzulässige Abhören von Wohnungen und Telefongesprächen, die Eingriffe in die Telekommunikation und verschiedene weitere polizeiliche Maßnahmen sind Gegenstand der Rechtsprechung des Gerichtshofes. Gleiches gilt für die Bild-

[1] Das Modul wurde im August 2009 mit dem EuroPriSe-Siegel (www.european-privacy-seal.eu) ausgezeichnet. Es ermöglicht im Einzelfall etwa die datenschutzgemäße Verschleierung von Video-Klardaten in Echtzeit. Bewegte Personen oder personenbeziehbare Objekte (z.B. Kfz-Kennzeichen) in digitalen Videobildern, die nicht erforderlich sind, können unkenntlich gemacht werden.

Überwachung des Personenverkehrs zu Wohnungen oder das elektronische Eindringen in diese.

Der Gerichtshof schafft in seiner Einzelfall-Judikatur **Distanz zu der Maßlosigkeit der Überwachungsvorgänge in europäischen Staaten**. Auch das Bundesverfassungsgericht hat beschämende Tiefpunkte in der Sicherheitsdebatte immer wieder reflektiert. Es hat auf den Möglichkeitshorizont der modernen Technik reagiert und ein IT-Grundrecht formuliert. Mit der Schaffung des neuen Grundrechts versucht das Gericht, sich einem Modell der „Freiheit für die Technik" der Bürgerin und des Bürgers anzunähern.

IV. Das IT-Grundrecht: Garant der Freiheit für die Technik?

Die vernetzte digitale Datenverarbeitung macht es möglich, noch mehr Informationen heimlich zu erlangen, sie beliebig zusammenzuführen, ohne dass Bürger und Bürgerinnen die Richtigkeit und Verwendung ihrer Daten kontrollieren könnten. Cyberkriminelle nutzen die Schutzlücken eigengenutzter IT-Syteme und überführen sie in ein sogenanntes Botnetz (Netz von Robotern), um sie wahlweise für das Versenden von Spam oder für gezielte Angriffe auf einzelne Dienste im Netz einzusetzen.

Sicherheitsbehörden haben ebenfalls damit begonnen, diese Einfallstore zu nutzen. Sie legen auch kein Stopp-Schild vor den Toren derjenigen ein, die aufgrund ihres Berufes zur Verschwiegenheit verpflichtet sind (z.B. Journalisten, Ärzte und Anwälte). Die Behörden durchsuchen mit technischen Hilfsmitteln, sogenannten „Trojanischen Pferden" (Online-Durchsuchung) privat genutzte Rechner, um heimlich **Informationen über die Lebensgestaltung** der jeweiligen (verdächtigen)" Zielperson" sowie ein aussagekräftiges Bild ihrer potenziellen terroristischen oder anderen kriminellen Pläne zu gewinnen.

Wer immer sich den **Zugang zu den IT-Systemen** der Bürger verschafft , erhält nach den Worten Winfried Hassemers - jedenfalls ausschnitthaft - **Zugang** zu deren **„ausgelagertem Hirn".** Er erhält die Möglichkeit, lebensbestimmende intime und private Informationen kennen zu lernen. Beim Zugriff auf solche Systeme droht zugleich ihre irreversible Manipulation. In seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 hat das Bundesverfassungsgericht die Konsequenz aus den neuen technischen Angriffspotenzialen im Internet und deren Verlagerung auf die eigengenutzten Rechner gezogen und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Das Gericht hat gleichzeitig anlasslosen Eingriffsinteressen der Vertreter von Polizei und Geheimdiensten einen Riegel vorgeschoben. Ihr Traum, eher am Tatort zu sein als der Täter, dürfte damit hoffentlich ein Ende gefunden haben.

An dem neuen **IT-Grundrecht** ist zwar nicht abzulesen, wie der angemessene Schutz der Grundrechtsträgerin/des Grundrechtsträgers im Einzelnen auszusehen hat. Immerhin steht fest, dass sie die **Technik frei und selbstbestimmt** nutzen können. Ohne Vertrauen in die eigene Technik sind sie fremden Eingriffen in ihr Privatleben und ihre Kommunikation ausgeliefert. So gesehen ist das Plädoyer von Ulrich Beck *„Freiheit für die Technik“* zur Bedingung des Überlebens für den Einzelnen sowie seine Kontakt- und Begleitpersonen in einer offenen Gesellschaft geworden. Dabei trifft den Rechtsstaat zweifellos die Aufgabe, diese Freiheit zu schützen, auch wenn sie von Dritten bedroht wird.

V. Schlussbetrachtung: Die Menschenwürde ist nicht wegwägbar

Wilhelm von Humboldt führte einst aus, dass *Sicherheit ohne Freiheit* unerträglich wäre. Dies hat auch das Bundesverfassungsgericht immer wieder betont und darüber hinaus ausdrücklich festgestellt, dass Eingriffe in den **Kernbereich privater Lebensgestaltung**, der sich letztlich aus der **Menschenwürde** ableitet, durch staatliche Überwachungsmaßnahmen nicht erlaubt werden. Die Menschenwürde ist **nicht wegwägbar**, auch nicht mit Sicherheitspflichten des Staates. Daher stellt sich bei der Online-Durchsuchung ein gravierendes Problem. Vor einer Datenerhebung kann nicht geklärt werden, ob persönlichste Informationen (Gedanken, ungestüme Phantasien, intime Aussagen usw.) aus dem Kernbereich betroffen sind. Wird damit nicht der unendlich wertvolle Vorrat an persönlichem Gedankengut bedroht? Haben nicht totalitäre Systeme Versuche in diese Richtung unternommen?

Um solche Bedrohungen des Kernbereichs abzuwenden, hat das Bundesverfassungsgericht ein zweistufiges Schutzkonzept durch die Unterscheidung von Erhebungs- und Auswertungsphase entwickelt. Dies hindert zwar die Sicherheitsbehörden, nicht aber einen kontrollierenden Richter, Kenntnis von Informationen aus dem Kernbereich zu erhalten. Damit aber wird nun der Kernbereich für die Abwägung durch den Richter offen und so auch antastbar oder sogar relativierbar.

Durch ständige Wiederholung einer Aussage im Sinne Catos wird schließlich Wahrheit vorgetäuscht. Ständige Hinweise auf die bedrohte Sicherheit lassen Anti-Terror-Gesetze ausufern. Dass sie ihre Grenze in der Unabdingbarkeit der Menschwürde finden, ist ein Postulat, das wir alle zu verteidigen haben.