Informationsgesellschaft, Sicherheit und Menschenrechte

Marie-Theres Tinnefeld

Hochschule München
tinnefeld@cs.hm.edu

Abstract: Das Thema behandelt zentrale Herausforderungen in der digital vernetzten Informationsgesellschaft, die eng mit der modernen Informationstechnik verbunden ist. Schutzmaßnahmen sind in verschiedene Richtungen notwendig, die Herbert Fiedler bereits frühzeitig angesprochen hat. Das Bundesverfassungsgericht hat die informationstechnische Entwicklung insbesondere durch die Einrichtung und Ausführung von zwei „neuen" Menschenrechten in grundrechtfreundliche Bahnen gelenkt: den Grundrechten auf Datenschutz (1983) und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (2008). Der Beitrag untersucht die Bedeutung dieser Menschenrechte in Zeiten des Terrors und der damit verbundenen Forderung nach immer mehr innerer Sicherheit. Er schließt mit der weisen Feststellung des Philosophen Baruch des Spinoza (1670), wonach der Zweck des Staates in Wahrheit die Freiheit ist.

1 Einführung

Das Thema "Informationsgesellschaft, Sicherheit und Menschenrechte" stellt sich am Beginn des 21. Jahrhunderts zentralen Herausforderungen unserer digital vernetzten Gesellschaft. Eine Analyse, der dadurch hervorgerufenen Veränderungen zeigt zwei gegenläufige, aber zusammenhängende Aspekte der modernen Informationstechnik. Zum einen entstehen neue Bedrohungen, zum anderen neue Rechte und Schutzmechanismen. Das mit der Nutzung der Informationstechnik Schutzmechanismen in verschiedene Richtungen notwendig geworden sind, hat Herbert Fiedler im Feld von Datenschutz und Datensicherheit schon frühzeitig erkannt und insbesondere die Systematik „informationeller Garantien eingefordert([FI94], S. 147-158).

Der internationale Terrorismus und die organisierte Kriminalität (OK) stellen den Rechtsstaat vor neue Sicherheits-Anforderungen.[1] Der vorliegende Beitrag versucht, den

[1] Zur Abgrenzung der OK von Straftaten des Terrorismus in Deutschland vgl. [KI09], S. 57ff.

dadurch bedingten Veränderungen in Staat und Gesellschaft nachzugehen. Der Staat hat sich auf eine Politik der inneren Sicherheit eingestellt, die weitreichende Eingriffe in die Privatsphäre und Kommunikationsfreiheitsrechte in Kauf nimmt. Diese Eingriffe werden von Politikern auf der nationalen, aber auch zunehmend auf der EU-Ebene als ein notwendiger Teil der Sicherheits-Fortentwicklung gewertet. Besonders fragwürdig ist dabei, dass die Überwachung persönlicher Datenverarbeitung und vertraulicher Telekommunikation durch die Sicherheitsbehörden für den betroffenen Bürger zunehmend „unsichtbar" erfolgt und in ihren Wirkungen undurchschaubar bleibt. Der wesentliche menschenrechtliche Aspekt, die „Sicherheit" privater und intimer Daten für den Betroffenen durch verfahrensrechtliche informationelle Garantien zu gewährleisten, bleibt weitgehend auf der Strecke.

Das deutsche Bundesverfassungsgericht hat die informationstechnischen Veränderungen mit Beginn der automatischen Datenverarbeitung analysiert und versucht, die neuen Entwicklung in grundrechtsfreundliche Bahnen zu lenken. Beginnend mit der Einrichtung und Ausführung des Grundrechts auf Datenschutz (1983)[2] bis zur Gewährleistung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (2008)[3] hat das Gericht den Schutz des Bürgers immer enger mit der Technik .kombiniert. Durch die Weiterentwicklung der modernen Informationstechnologie seien insbesondere dem Staat Machtdimensionen zugewachsen, die den Bürger in eine Verletzungsgefahr bringe, welche bislang in einer solchen Dimension nicht existiert habe. Die Entscheidung von 2008 ist auch das Ergebnis einer langjährigen Auseinandersetzung des Gerichts über Art, Umfang und Auswirkung heimlicher Ermittlungsmethoden mit technischen Hilfsmitteln. Die Fähigkeit des Rechts, soziales Vertrauen zu begründen und Verhaltenssicherheit zu schaffen, wird angesichts heimlicher Überwachungsmethoden mit (unsichtbaren) technischen Mitteln stark herabgesetzt. Die Bedrohungen erschweren nachhaltig die selbstbestimmte Lebensführung und offene Kommunikation in der Informationsgesellschaft.

1.1 Informationsgesellschaft

Das Schlagwort der Informationsgesellschaft beschreibt in den Wirtschaftswissenschaften eine Gesellschaft, in der immaterielle Informationen und nicht körperliche Gegenstände zu maßgeblichen Produktionsfaktoren geworden sind. Durch das Aufnehmen und Verknüpfen von Informationen „schafft der Mensch in seinem Kopf neues Wissen, d.h. es findet ein Lernprozess statt. Wissen ist also immateriell, intangibel (nicht greifbar). Wenn es dem Menschen dann gelingt, sein neues Wissen in Worte zu fassen, produziert er wieder Daten([HA07], 33 ff). Diese Daten

[2] BVerfG 63, 1 – Volkszählungsurteil.
[3] 1 BvR 370/07 und 1 BvR 595/07.

können in informationstechnischen Systemen gespeichert werden, z.B. in Datenbanken und Internet. Dabei kommt der Entwicklung und Nutzung von Information als auch deren Richtigkeit und Verfügbarkeit eine entscheidende Bedeutung zu. Manipulationen etwa in Zahlungssystemen oder in Sicherheitsüberwachungssystemen von Staat und Wirtschaft können gravierende Auswirkungen auch auf den Persönlichkeitsschutz haben. Es ist keineswegs trivial, wenn man in der Informationsgesellschaft der Perspektive des Datenschutzes eine wesentliche Bedeutung einräumt. Das Datenschutzrecht soll Informationsflüsse lenken und nicht verhindern. In dieser Betrachtungsweise ist die Gestaltung des Datenschutzes eine Art Steuermannskunst, die das Recht auf Privatheit auch in Zeiten des Terrors sichert. Die Festplatte des persönlichen PCs darf als ein virtuelles Spiegelbild des Nutzers nicht von Trojanern überwältigt werden!

Das Bundesverfassungsgericht hat den herausragenden Rang der Sicherungstechnik für den Schutz des Betroffenen erkannt und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen.[4] An dieser Stelle lässt sich im Sinne der Rechtsinformatik mit den Worten Fiedlers formulieren, dass Informationstechnik einerseits als Hilfsmittel des Rechts und andererseits als Gestaltungsprinzip der Informationstechnik und informationstechnischer Systeme gesehen werden muss([FI94], S.148).

1.2 Sicherheit

Die informationstechnischen Bedrohungen der inneren Sicherheit in der Informationsgesellschaft werden häufig mit dem Begriff der Computerkriminalität umschrieben, wozu in der Wirtschaftskriminalität Computerbetrug, Computerspionage oder Hacking gehören. Neuere Untersuchungen belegen, dass es neben Spyware und Bot-Netzen[5] eine deutliche Zunahme bei der Verbreitung von Trojanischen Pferden oder umgangssprachlich kurz Trojanern gibt. Technologisch gesehen bedeutet dies, „dass mit dem fortschreitenden Einsatz des Internets auch die verschiedenen technischen Schadszenarien zugenommen haben“([HE08], S. 8f). Die vernetzte Welt ist risikoreicher geworden.

Das Stichwort Risikogesellschaft, das Ulrich Beck für die Soziologie geprägt hat, charakterisiert den Entwicklungsstand einer Gesellschaft, die nicht nur im Bereich der Informationstechnik, sondern allgemein durch größere Technikrisiken gekennzeichnet ist. Zwar ist die Technik auf der einen Seite „zur Bedingung der Möglichkeit des Überlebens“, auf der anderen Seite aber zu einer „alle Lebensbereiche permanent

[4] 1 BvR 370/07 und 1 BvR 595/07, Abs. 181.

[5] Computer-Netze, die aus unbemerkt ferngesteuerten PCs bestehen, die zu Angriffen auf die IT von Unternehmen und Organisationen eingesetzt werden.

umwälzenden politischen Kraft (...) ersten Ranges“ geworden([BE94], S. 13 ff).

Terroristen haben mit ihren Attentaten die Parlamente demokratischer Rechtsstaaten dazu gebracht, Menschenrechte für Sicherheitszwecke massiv einzuschränken, vor allem den Datenschutz und die Kommunikationsgrundrechte. Viele Bürger tragen aus Angst vor dem Terror Gesetze mit, die ihre eigenen Bewegungsspielräume empfindlich begrenzen. Auf dem grundrechtlichen Prüfstand stehen aktuell Gesetze zur Vorratsdatenspeicherung und zur Online-Durchsuchung.

2 Vorratssammlung von TK-Verkehrsdaten

Die Europäische Union hat im Jahr 2006 eine Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) verabschiedet. Es ist umstritten, ob die EG für eine Regelung, die der Identifizierung von Straftätern dient, überhaupt die erforderliche Kompetenz hat. Der einheitliche Wettbewerbsrahmen der EG (1. Säule der EU) ist zwar berührt, weil die Richtlinie die Provider aller Mitgliedstaaten zur Speicherung von Verkehrsdaten verpflichtet. Eine andere Sichtweise ergibt sich jedoch hinsichtlich der Verwendung der Daten durch die Sicherheitsbehörden (3. Säule der EU)([TI05], S. 113 ff). Die Kompetenzfrage würde sich nach einer Ratifizierung des Reformvertrags von Lissabon (2007)[6] durch die EU-Mitgliedstaaten nicht mehr stellen, weil sie auch das Ende des Drei-Säulen-Modells und der aufgespalteten Kompetenzen bedeuten würde (Art. 1 Abs. 3 EUV). Im Übrigen ist aber auch die Frage offen, ob die Maßnahme als solche verhältnismäßig ist.

Die Richtlinie erlaubt den Ermittlungsbehörden keine Inhaltskontrolle, wohl aber die näheren Umstände der Telekommunikation zu erforschen und die TK-Nutzungs- und Verbindungsdaten bei den TK-Dienstleistern anzufordern und abzuspeichern. Dabei geht es um die Frage: Wer hat mit wem, wann, wie lange von wo nach wo fernmündlich oder schriftlich kommuniziert, welche SMS- oder Internetverbindung genutzt? Die Datensammlung unter der Mitwirkung des privaten Dienstanbieters weist eine erhebliche Streubreite auf; sie erfasst das soziale Umfeld der Betroffenen und erstreckt sich auch auf völlig unverdächtige Kommunikationsteilnehmer.

Die Richtlinie wurde unter anderen auch von Deutschland umgesetzt. Die angeordneten Maßnahmen bedeuten einen tiefen Eingriff in das verfassungsrechtlich geschützte Fernmelde- bzw. Telekommunikationsgeheimnis (Art. 10 I GG; s.a. Art. 8 EMRK). Lässt sich mit ihnen das angestrebte Ziel, die Identifizierung von Straftätern erreichen? Mit anderen Worten: Sind sie verhältnismäßig? Das Bundesverfassungsgericht hat am

[6] http://eur-lex.europa.eu/JOHtml.do?uri=OJ.C:2008:115:SOM:EN:HTML.

11.3.2008 im Verfahren des Eilrechtsschutzes entschieden, dass sie nur für bestimmte Zwecke, nämlich für die Verfolgung schwerer Straftaten[7] genutzt werden dürfen.[8] Die Richtlinie wäre dann zwar hinreichend bestimmt. Kann aber die Maßnahme als solche nicht „zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen (...)“[9] bei den betroffenen Bürgern führen?

Bei einer flächendeckenden Datenspeicherung auf Vorrat werden immer auch sensible Kontakte zu Ärzten, Journalisten, Rechtsanwälten und Abgeordnete mit Informanten, Mandanten und Patienten über einen längeren Zeitraum rekonstruierbar. Damit ist der Schutz besonderer Vertrauensverhältnisse gefährdet. Selbst zum Schutz gewichtiger Rechtsgüter wie dem Schutz der inneren Sicherheit können Eingriffsgesetze keinen Bestand haben, wenn sie mit unverhältnismäßigen Nebenfolgen verbunden sind.[10] Betrachtet man die neuesten Skandale bei Lidl & Co, dann wecken die Vorratsspeicher der Provider Begehrlichkeiten, die zum Missbrach personenbezogener Daten in der Privatwirtschaft verleiten.[11] Die Vorgänge bei der Telekom zeigen nicht nur wie groß das Informationspotential der Provider über den einzelnen Bürger ist, sondern auch, dass es sich um eine ökonomisch vielfältig verwendbare Verfügungsmasse handelt.

Der Zugriff des deutschen Gesetzgebers auf die Grundrechte wird auch durch die Wesengehaltsschranke (Art. 19 Abs. 2 GG) begrenzt. Der unantastbare Wesensgehalt eines Grundrechts ist aus seiner besonderen Bedeutung im Grundrechtssystem der Grundrechte zu ermitteln.[12] Er ist beeinträchtigt, wenn eine im Grundgesetz verankerte, der Allgemeinheit gegebene Freiheitsgarantie angetastet wird.[13] Das ist hier der Fall. Das Fernmeldegeheimnis soll die Vertraulichkeit individueller Kommunikation sicherstellen, die wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch Dritte angewiesen sind.[14] Der Staat soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informationen zu verschaffen. Hierunter ist auch die Erlangung der Kenntnis zu verstehen, ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist.[15] Ein Eingriff in das TK-Geheimnis durch die Datenerhebung setzt sich mit der Speicherung der Daten durch die Provider fort, durch die das Material aufbewahrt und für den Zugriff der

---

7 Katalogtaten des § 100a Abs. 2 StPO.

8 BVerfGE, 1 BvR 256/08 v. 11.3.2008, Abs.-Nr. 164ff.

9 BVerFGE 100 313, 381; 65, 1, 43.

10 BVerfGE 100, 51, 101.

11 Zur Ahndung vgl. unter: https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf.

12 Vgl. zur Bedeutung der Wesensgehaltssperre [GR01], S.98f, siehe auch BVerfGE 109, S. 133, 156 m.w.N.; BVerfGE 22, S. 180, 219.

13 Vgl. bereits BVerfGE 2, 266, 285, seither st. Rspr.

14 Vgl. BVerfGE 106, 28, 36; BVerfGE 100, S. 313, 366; BVerfGE 85, 386, 396.

15 Vgl. BVerfGE 113, 348, 364 f.; BVerfGE 100, 313, 358.

Ermittlungsbehörden bereitgehalten wird.[16]

Die Folgen einer Verletzung der Wesensgehaltsgarantie auf europäischer Ebene können hier nicht vertieft werden. Nach der Maastricht-Entscheidung des Bundesverfassungsgerichts[17] kann das deutsche Gericht prüfen, ob sich die Rechtsakte der EG an ihre kompetenzrechtlichen Grenzen halten.[18] Das Gericht hat die Streitfrage dem EuGH zur Entscheidung vorgelegt.[19]

Schon im Volkszählungsurteil hat das Bundesverfassungsgericht notwendige fundamentale Beschränkungen staatlicher Informationsverarbeitung formuliert. Dazu gehören flankierende prozedurale Schutzvorkehrungen, die Fiedler immer besonders betont hat.

3 Online-Durchsuchung

Eine neue eingriffsintensive Maßnahme im Kampf gegen Terror und OK ist der heimliche Zugriff von Sicherheitsbehörden auf informationstechnische Systeme. Die Maßnahme wird auch als Online-Durchsuchung definiert.[20] Sie ist als solche nicht ganz neu,[21] erhält aber durch verdeckte Angriffe über Internetverbindungen, über die Installation von Schadprogrammen bzw. Trojanern eine neue Eingriffsqualität.

Trojaner werden durch ungesicherte Einfallstore von Betriebssystemen, über Mailanhänge oder über Programmdownloads von präparierten Websites eingeschleust. Sie sind in der Lage, unbemerkt den infizierten Inhalt der Festplatte zu kopieren, um ihn dann via Internet an die Sicherheitsbehörden zur weiteren Ausforschung bzw. für weitere Ermittlungs- und Aufklärungsarbeiten zu senden.

Zu Recht erinnert Andreas Pfitzmann daran, dass sich gespeicherte Computerdaten an vielfältigen Stellen finden:

- Server,
- Persönliche Rechner (wie Desktop, Laptop, PDA, Smartphone, Mobiltelefon) in Wohnung, Rucksack, Jackett oder Handtasche, „sondern teilweise bereits heute, zukünftig zunehmend, in unserem Körper:
- Herzschrittmacher, Hörhilfen, zukünftig

16 Vgl. BVerfGE 100, 313, 366.
17 BVerfGE 89, 155 ff.
18 Vgl. BVerfGE 89, 155, 188.
19 Rs. C-301/06.
20 BVerfG 1 BvR 370/07 und 1 BvR 595/07
21 Vgl. BGH-Ermittlungsrichter, NJW 1997, 1934 ff.

- Erinnerungs- und Denkhilfe.“

Aufgrund der technischen Entwicklung „wird Freiheit und Unbeobachtbarkeit des Denkens (etwa beim Erwägen von Äußerungen und Handlungen) künftig untrennbar mit dem Schutz persönlichster Rechner, ihrer Anwendung auch der Daten auf ihnen verknüpft sein [PF07]. Die Computerdaten im PC oder in vergleichbaren technischen Systemen können mit einer Art ausgelagertem Hirn (Burkhard Hirsch) verglichen werden. Der heimliche Zugriff auf die Daten ermöglicht die Ausforschung des Denkens, der persönlichen Meinungen und der Privatsphäre. Er nähert sich Eingriffen in Leben und Körper des betroffenen Bürgers und verletzt dessen Privatheit. Je nach den äußeren Umständen kann der Eingriff auch mit einer Verletzung des Rechts auf Unverletzlichkeit der Wohnung (Art. 13 GG) verbunden sein, muss es aber nicht.[22]

Nach den Feststellungen des Gerichts trägt das "Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht hinreichend Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungen und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus."[23]

In seiner Entscheidung legt das Gericht den Schwerpunkt auf den technischen System-Aspekt. Es verbindet die Sicherheit des Systems mit dem verfassungsrechtlichen Schutz des Nutzers, unabhängig davon, ob konkret eine personenbezogene Datenverarbeitung stattgefunden hat. Datensicherheit war zwar schon immer schon immer ein integraler Bestandteil des europäischen Datenschutzes (vgl. Art. 17 EG Richtlinie (95/46/EG). Sie greift aber erst bei einer Verarbeitung persönlicher Daten. Der Aspekt des Systemschutzes als solcher ist also neu.

Dem Bürger kommt hier wie in jedem Verfahren der Rechtsanwendung ein Recht auf Anhörung und Mitwirkung zu. Von erheblicher Bedeutung ist sein Recht auf Auskunft über die Daten, die der Staat im Rahmen der heimlichen Überwachungsmaßnahme hinsichtlich seiner Person erfasst und gespeichert hat. Unter Umständen kann die Benachrichtigung auch nachträglich erfolgen, wenn auf Grund der Kenntnis des

[22] BVerfG, 1 BvR 370/07 und 1 BvR 595/07, Abs. 193.
[23] BVerfG a.a.O,. Abs. 200.

Betroffenen eine zulässige Überwachungsmaßnahme ihren Zweck verfehlen würde.[24]

3.1 Menschenrechte

Die Menschen- und Grundrechte (beide Begriffe werden hier synonym verwandt) in Europa knüpfen an die Allgemeine Erklärung der Menschenrechte der Vereinten Nationen an, die auch die Basis für die Europäische Menschenrechtskonvention (EMRK) ist, deren Bestimmungen sich nahezu wortgleich in der noch nicht rechtswirksamen EU-Charta der Grundrechte wiederfinden. Ergänzend zu der EMRK sieht aber die Charta explizit ein Grundrecht auf Schutz personenbezogener Daten vor. Dies lässt auf die dynamische Bedeutung der Grundrechte schließen. Andernfalls wäre das Grundrechtsverständnis statisch und böte unter Umständen keinen ausreichenden Schutz. Das Bundesverfassungsgericht hat bei Freiheitsgefahren, die neuer sind als das Grundgesetz, weitere Grundrechte formuliert. In der Informationsgesellschaft sind vor allem die Rechte von Bedeutung, die das Gericht unter den Bedingungen der neuen Technologien aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) entwickelt hat. Dazu gehören:

- Das Grundrecht auf Datenschutz[25] und
- das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[26]

Im Datenschutzrecht gibt es eine Reihe von materiellen Grundsätzen (z.B. den Grundsatz der Zweckbindung, Pflichten der Aufklärung usw.), die das Selbstbestimmungsrecht des Bürgers jenseits staatlicher, aber auch privater Einschüchterung stabilisieren sollen. Rechtsgrundsätzlich von zentraler Bedeutung ist im Grundrechtsschutz das Prinzip der Verhältnismäßigkeit. Unverhältnismäßige Eingriffe verletzen nicht nur die Grundrechte des betroffenen Bürgers, sondern sind auch das Gegenbild einer rechtsstaatlichen Staatstätigkeit. Erst bei der Anwendung des Rechts fällt die Entscheidung über den konkreten Freiheitsraum des Einzelnen.

In ständiger Rechtsprechung hat das Bundesverfassungsgericht immer wieder darauf hingewiesen, dass der Staat bei heimlichen Überwachungsmaßnahmen einen unantastbaren Kernbereich privater Lebensgestaltung zu respektieren hat.[27] Eingriffsintensive Maßnahmen sind nur hinnehmbar, wenn gleichzeitig taugliche, geeignete und angemessene Mechanismen zur Sicherung des Schutzes Einzelner

[24] BVerfGE 100, 313, 366.
[25] BVerfGE 65, 1.
[26] 1 BvR 370/07 und 1 BvR 595/07.
[27] Ständige Rechtsprechung, BVerfGE 109, 279, 313 m.w.N.

geschaffen werden.

Der neuralgische Punkt beider Online-Durchsuchung ist die verfassungsrechtliche Forderung, den Kernbereich privater Lebensgestaltung nicht zu berühren. Will der Gesetzgeber zuverlässig die Verwendung kernbereichsrelevanter Daten ausschließen, dann kommt für die Sichtung entsprechender Daten eine Ermittlungsbehörde nicht in Frage. Die Sichtung durch einen Richter würde zwar Missbrauchsgefahren reduzieren, der absolute Kernbereich wäre aber nur bedingt gegen dein Einblick Dritter abgeschottet.[28]

Zu den wesentlichen Forderungen der Menschenrechte gehört es immer, dass der Betroffene über heimliche Ermittlungsmaßnahmen benachrichtigt wird; nachträgliche Informationen sollten innerhalb einer verbindlichen Maximalfrist erfolgen.

4 Conclusio

In einer bemerkenswerten Rede hat der Präsident des Bundesverfassungsgerichts, Jürgen Papier, die erforderliche Balance von Freiheits- und Sicherheitszwecken im Staat eingefordert.[29] Papier hat seinen Ausführungen Worte des niederländischen Philosophen Baruch de Spinoza aus dem Jahre 1670 vorangestellt: „Der letzte Zweck des Staates ist nicht zu herrschen noch die Menschen in Furcht zu halten oder sie fremder Gewalt zu unterwerfen, sondern vielmehr den einzelnen von der Furcht zu befreien, damit er so sicher als möglich leben und sein natürliches Recht zu sein und zu wirken ohne Schaden für sich und andere vollkommen behaupten kann. Der Zweck des Staates ist in Wahrheit die Freiheit.“[30]

Größere Technikrisiken und neue Bedrohungen in der Informationsgesellschaft können nur anhand verfassungsrechtlicher Maßstäbe gemeistert werden. Die Interpretation der grundrechtlichen Freiheit des Bürgers ist an der Verhältnismäßigkeit von Maßnahmen wie der Vorratsspeicherung oder der Online-Durchsuchung (Mittel) und ihrer Zwecke (Zweck-Mittel-Relation) zu orientieren. Nur so kann die Balance zwischen Freiheit und Sicherheit jeweils neu justiert werden.

Die Gewichte dürfen sich in einer offenen Gesellschaft auch in Zeiten des Terrors nicht grundlegend verschieben. Selbst zum Schutz gewichtiger Rechtsgüter können

---

[28] Dazu grundsätzlich [PE08], S. 447.

[29] Papier, Der Zweck des Staates ist die Wahrung der Freiheit. Über das Spannungsverhältnis von Freiheit und Sicherheit aus verfassungsrechtlicher Sicht – Ein Vortrag auf der Tagung „Freiheit und Sicherheit – Verfassungsrechtliche Dimensionen“ in der Akademie für Politische Bildung Tutzing am 30. Mai 2008, zugänglich unter: http://www.welt.de/papier.

[30] Spinoza, Tractatus Theologico-politicus (1670), 20.

Eingriffsgesetze keinen Bestand haben, wenn sich nach Ablauf einer gewissen Frist herausstellt, dass sie ganz oder teilweise auf unzulässigen Prognosen beruhen oder mit unzumutbaren Nebenfolgen verbunden sind. Den Gesetzgeber treffen mit anderen Worten, Beobachtungs- und Nachbesserungspflichten.

Andreas Pfitzmann fragt ganz konkret, ob Terroristen und andere Kriminelle keine Alternativen zur Nutzung des Internets haben, so dass Bedarfsträger auf die Online-Untersuchung angewiesen seien. Er weist daraufhin, dass im militärischen Bereich „Funktechniken nach dem Prinzip Spread-Spectrum bekannt sind, die unterhalb der Rauschschwelle bleiben und von Außenstehenden nicht detektiert und gepeilt werden können“ [PF07]. Wenn das Internet für die Sicherheitsbehörden kontrollierbar ist, warum sollten Kriminelle dann nicht auf diese Geräte ausweichen?

Die Regeln grundrechtlicher Freiheitssicherung hat vor allem das Bundesverfassungsgericht auch in Zeiten des internationalen Terrors und der organisierten Kriminalität aufrechterhalten Das zeigt sich exemplarisch an der Einrichtung und Ausführung der neuen Menschenrechte. Zum wirksamen Schutz dieser Rechte sind immer auch prozedurale Vorkehrungen erforderlich. Es ist ein besonderes Verdienst des Rechtsinformatikers Herbert Fiedler, dass er verfahrensrechtliche und organisatorische Vorkehrungen zur Sicherung von Grundrechten, ein notwendiges System informationeller Gewährleistung, frühzeitig in das verfassungsrechtliche Rampenlicht gerückt hat.

Literaturverzeichnis

[HE08] Helmbrecht, in: Helmbrecht/Thielmann/Ziemer (Hg), Elektronischer Personalausweis und E-Identity, 2. Berliner Gespräch, Münchner Kreis, 2008, 8f.

[GR01] Grimm, Dieter: Die Verfassung und die Politik, C. H. Beck Verlag, München 2001

[BE94] Beck, Ulrich: Freiheit für die Technik! Plädoyer für eine zweite Gewaltenteilung. In Tinnefeld Marie-Theres/Philipps Lothar, Weis Kurt (Hrsg.): Institutionen und Einzelne im Zeitalter der Informationstechnik. R. Oldenbourg Verlag, München Wien, 1994, 13-18.

[FI94] Fiedler, Herbert: Informationelle Garantien für das Zeitalter der Informationstechnik. In Tinnefeld Marie-Theres/Philipps Lothar, Weis Kurt (Hrsg.): Institutionen und Einzelne im Zeitalter der Informationstechnik. R. Oldenbourg Verlag, München Wien, 1994, 147-157.

[HA07] Hasler Roumois: Studienbuch Wissensmanagement. Grundlagen der Wissensarbeitin Wirtschafts-, Non-Profit und Public-Organisationen, Zürich 2007.

[KI04] Kinzig Jörg: Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, Duncker & Humblot Berlin 2004.

[PE08] Petri Thomas: Das Urteil des Bundesverfassungsgerichts zur "Online-Durchsuchung". In: DuD Heft 7, 2008, 443-448.

[PF07] Pfitzmann, Sprechzettel vor dem Bundesverfassungsgericht zur Online-Durchsuchung: BVG2007.10.10.pdf unter: http://www.inf.tu-dresden.de/index.php?node_id=703&ln=de

[TI05] Tinnefeld, Marie-Theres, Ehmann Eugen, Gerling Rainer, Einführung in das Datenschutzrecht, R. Oldenbourg Verlag München Wien, 4. Auflage, 2005.