FAU Forschungen, Reihe A, Geisteswissenschaften 3

Datenschutz – aktuelle Fragen und Antworten

Atzelsberger Gespräche 2014

Herausgegeben von Helmut Neuhaus

FAU UNIVERSITY PRESS

Datenschutz – aktuelle Fragen und Antworten

Atzelsberger Gespräche

FAU Forschungen, Reihe A, Geisteswissenschaften
Band 3

Datenschutz - aktuelle Fragen und Antworten

Atzelsberger Gespräche 2014

herausgegeben von Helmut Neuhaus

Erlangen
FAU University Press
2015

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Frontipiz: Zuhörer während der Atzelsberger Gespräche am 4. Juli 2013;
Foto: Andreas Jakob. Entnommen dem Buch „Schloß Atzelsberg in drei Jahrhunderten“, hrsg. von Johann Schorr, Erlangen 2013, Seite 41
(ISBN 978-3-944452-02-9).

Umschlaggestaltung: Stefan Dinter, unter Verwendung eines Ausschnitts aus der Farblithographie „Atzelsberg“ von Gerhard Schmid-Kaler (1950. Stadtarchiv Erlangen, VI.T.a.560).

Wir bedanken uns für die freundliche Unterstützung durch:

Der vollständige Inhalt des Buchs ist als PDF über den OPUS Server der Friedrich-Alexander-Universität Erlangen-Nürnberg abrufbar:
http://opus.uni-erlangen.de/opus/

Verlag und Auslieferung:
FAU University Press, Universitätsstraße 4, 91054 Erlangen

Lasersatz: NIELAND, Textverarbeitung, Baiersdorf

Druck: 6ÅÒÌÁÇÓÄÒÕÃËÅÒÅÉ 3# (-)$ 4ǩ . ÅÕÓÔÁÄÔ! ÉÓÃÈ

ISBN: 978-3-944057-31-6

ISSN: 2199-014X

Inhaltsverzeichnis

Vorwort

Nicht erst seit den Enthüllungen Edward Snowdens, eines ehemaligen US-Geheimdienst-Mitarbeiters, war „Datenschutz“ zu einem großen Thema unserer Zeit geworden. Aber seit Juni 2013 beschäftigte es die nationale wie internationale Öffentlichkeit in einem bisher nicht gekannten Ausmaß. Es wurde zu einem täglich immer wiederkehrenden Bestandteil unserer Nachrichten in allen ihren Erscheinungsformen. Nicht nur, aber vor allem eine von einer Vielzahl internationaler Autoren verfaßte Artikelserie der „Frankfurter Allgemeinen Zeitung“ hat in der ersten Hälfte des Jahres 2014 für mehr als nur publizistisches Aufsehen gesorgt. Weit über die Fragen hinaus, was mit unseren Kaufgewohnheits-, Bewegungs- oder Gesundheits- beziehungsweise Krankheitsdaten geschieht, die wir in der Regel nie ausdrücklich zur Verbreitung und Verwendung freigegeben haben, wurden grundsätzliche Probleme von „Big Data“ thematisiert. Neben der us-amerikanischen National Security Agency (NSA) rückten die uns allen bekannte Suchmaschine „Google“ sowie die Verbindungen von Nachrichtendiensten und privaten Suchmaschinen – Google mit einem Marktanteil von etwa 95 % weltweit – in bisher nicht gekannter Weise ins Zentrum der medialen wie individuellen Aufmerksamkeit.

Zugleich nutzt der Mensch alle digitalen Medien in immer noch größer werdendem Umfang. Dabei ist es angesichts einer nicht nur den Deutschen nachgesagten Empfindlichkeit gegenüber Eingriffen in das persönliche Leben bemerkenswert, daß in der andauernden Datenschutz-Debatte bisher eine breite Empörung gegen eine immer wieder beschriebene „Totalüberwachung“ mit ihren politischen und gesellschaftlichen Folgen sowie den Konsequenzen für Freiheitsverständnis und Menschenbild ausgeblieben ist. Das Handy und das Internet wird von fast jedem weiter mit Daten aller Art gefüttert, die freilich der Preis für die nur vermeintlich kostenlosen Nutzungsmöglichkeiten sind: Einlagen in Datenbanken generieren ein Vielfaches an Gewinnen im Vergleich zu Bankkonten – seit einigen Jahren allemal.

Darüber hinaus ist es bemerkenswert, wie lange es dauert, um neue gesetzgeberische Maßnahmen zu ergreifen, die vielleicht doch für mehr Datenschutz und Datensicherheit sorgen. Dabei ist nicht zu übersehen, daß Ländergrenzen für die digitale Verbreitung von Daten keine Schutzwälle sind und daß selbst schon in Europa schwer zu erzielende Vereinba-

rungen für die ganze Welt noch lange unzureichend bleiben müssen – bezogen auf ein globales Medium. Die Politik, ja die internationale Politik insgesamt ist gefragt, auch wenn deren zukünftige Antworten wohl immer schon zu spät sein werden, weil sich der Geist nicht mehr in die Flasche zurückbringen läßt.

Vor dem Hintergrund dieses riesigen Gesamtproblems unserer Zeit ging es bei den 33. Atzelsberger Gesprächen der Dr. Alfred-Vinzl-Stiftung an der Friedrich-Alexander-Universität Erlangen-Nürnberg am 3. Juli 2014 allerdings lediglich um „aktuelle Fragen und Antworten" zum „Datenschutz", die in drei Vorträgen deutlich gestellt, vorsichtig gegeben und lebhaft diskutiert wurden. Leider mußte der Eröffnungsvortrag des Historikers Professor Dr. Josef Foschepoth, Universität Freiburg im Breisgau, entfallen, dessen 2012 zuerst erschienenes, inzwischen in 4. Auflage vorliegendes Buch „Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik" großes Aufsehen erregt und ein breites Medienecho erfahren hat. Dankenswerterweise hat der Autor sein Vortragsmanuskript für die Drucklegung der „Atzelsberger Gespräche 2014" zur Verfügung gestellt, sodaß die Gesamtkonzeption der letztjährigen Veranstaltung in vorliegendem Band erkennbar wird.

Nach Foschepoths Beitrag über „Verfassung und Wirklichkeit" am Beispiel der „Überwachung des Post- und Fernmeldeverkehrs in der Geschichte der Bundesrepublik Deutschland" wendet sich der Erlanger Völkerrechtler Markus Krajewski den umfassenden „Völker- und menschenrechtliche[n] Anforderungen an Informationsbeschaffung und Datenüberwachung durch ausländische Geheimdienste" zu. Der Nürnberger Steuerrechtler Roland Ismer behandelt nicht nur vor dem Hintergrund des Ankaufs von „Steuer-CDs", die in der Schweiz illegal kopiert wurden, das Thema „Datenschutz im Steuerrecht", und schließlich stellt Thomas Kranig unter dem Titel „Datenschutz und Datensicherheit – mission impossible?" in einem breiten Kontext auch das in Ansbach ansässige und in Deutschland singuläre Bayerische Landesamt für Datenschutzaufsicht vor, dem er als Präsident vorsteht.

Ich danke allen Referenten und Autoren dafür, daß sie ihre Atzelsberger Vorträge für die Drucklegung und zur elektronischen Verbreitung – mit Anmerkungen und Literaturhinweisen versehen – überarbeitet zur Verfügung gestellt haben.

Herzlichen Dank sage ich auch in diesem Jahr wieder der EMZ-Hanauer GmbH & Co, Nabburg, und hier insbesondere Herrn Dipl.-Ing.

Ernst Hanauer, dem langjährigen Vorsitzenden und heutigen Ehrenvorsitzenden des Stiftungsrates der Dr. Alfred-Vinzl-Stiftung, sowie dem GfK-Nürnberg e.V., Nürnberg, vertreten durch Herrn Vizepräsidenten Professor Dr. Raimund Wildner, Herrn Gunther Oschmann vom Telefonbuch Verlag H. Müller GmbH & Co. KG, Nürnberg, und Herrn Diplom-Kaufmann Johann Schorr, Erlangen, dem Eigentümer von Schloß Atzelsberg, für die großzügigen finanziellen Zuwendungen zu den „Atzelsberger Gesprächen" des Jahres 2014. Ihre seit Jahren immer wieder oder erstmals gewährten Unterstützungen erlauben es neben zusätzlichen eigenen Anstrengungen der Stiftung, die Veranstaltung weiterhin in der zur Tradition gewordenen Form eines Symposions durchzuführen, ohne daß am Förderprogramm der Dr. Alfred-Vinzl-Stiftung Abstriche gemacht werden müssen.

Von Anfang an, d. h. seit 1979 sind die „Atzelsberger Gespräche" in der „Reihe A, Geisteswissenschaften", der „Erlanger Forschungen" im Verlag des Universitätsbundes Erlangen-Nürnberg e. V., Erlangen, publiziert worden, betreut von Mitarbeiterinnen und Mitarbeitern der Universitätsbibliothek Erlangen, zuletzt 2013 – allerdings schon im neuen Erlanger Verlag FAU University Press – als Band 127 die „Atzelsberger Gespräche 2012" zum Thema „Demokratie – Hoffnung und Krise". Mit vorliegendem Band wird die neue Reihe „FAU Forschungen, Reihe A, Geisteswissenschaften" in neuem Gewand fortgesetzt und darin die Folge der Publikationen der „Atzelsberger Gespräche".

Ein herzlicher Dank gebührt dem Wissenschaftlichen Beirat der FAU University Press für die Aufnahme auch dieses Bandes der „Atzelsberger Gespräche" in die neue Reihe sowie erneut Frau Beate Gresser von der Universitätsbibliothek Erlangen-Nürnberg für ihre verlegerische Betreuung. Zu danken ist schließlich einmal mehr Frau Ursula Nieland vom Satzbüro Nieland, Baiersdorf-Hagenau, und der Druckerei für die erneut gute Zusammenarbeit.

Erlangen, im April 2015

Für den Vorstand der
Dr. Alfred-Vinzl-Stiftung
Univ.-Prof. (em.) Dr. Helmut Neuhaus

Verfassung und Wirklichkeit: Die Überwachung des Post- und Fernmeldeverkehrs in der Geschichte der Bundesrepublik Deutschland[1]

JOSEF FOSCHEPOTH

Die Grundrechte im Grundgesetz

Das Grundgesetz der Bundesrepublik Deutschland gilt als die beste Verfassung, die die Deutschen jemals hatten. Zwar griffen die Siegermächte hier und da ein, aber im Ergebnis machten die (West-) Deutschen die Arbeit selbst. Der „Verfassungskonvent" vom Herrenchiemsee hatte innerhalb von 14 Tagen im August 1948 einen „Verfassungsentwurf" vorgelegt. Dieser diente als Vorlage für die „Verfassunggebende Versammlung" der 65 Delegierten aus den westdeutschen Landtagen. Vier Jahre nach der bedingungslosen Kapitulation, am 8. Mai 1949, verabschiedete der Parlamentarische Rat mit großer Mehrheit das Grundgesetz der Bundesrepublik Deutschland.

Zum ersten Mal bekam ein deutscher Staat eine Verfassung, in der die Menschen- und Grundrechte einen hohen und breiten Rang einnahmen. So lautet der erste Artikel wie folgt: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Das deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt. Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht."[2]

Die Grundrechte stehen über dem Staat und sind unmittelbar geltendes Recht. Aufgrund ihres vorstaatlichen und überpositiven Charakters kön-

1 Die folgenden Ausführungen basieren auf meinem Buch: Josef Foschepoth, Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik, 4. Auflage Göttingen 2014.

2 Grundgesetz (GG), Art. 1, Abs. 1-3.

nen und dürfen sie nicht abgeschafft werden.[3] Einige von ihnen können zwar durch ein allgemeines Gesetz, nicht aber in ihrem Wesensgehalt eingeschränkt werden.[4] Werden sie verletzt, können Sie von Jedermann auf dem Rechtsweg bis zum Bundesverfassungsgericht eingeklagt werden.[5] Eine Aberkennung von Grundrechten ist zwar möglich, faktisch aber auf Ausnahmefälle begrenzt. Nur wer die Grundrechte „zum Kampfe gegen die freiheitliche demokratische Grundordnung missbraucht, verwirkt diese Grundrechte. Die Verwirkung und ihr Ausmaß werden durch das Bundesverfassungsgericht ausgesprochen."[6] Eine Verwirkung von Grundrechten hat das höchste deutsche Gericht trotz verschiedener Verfahren in seiner über sechzigjährigen Geschichte nicht ein Mal ausgesprochen.

Rechtsstaatlich im „materiellen Sinn", wie Juristen sagen, ist eine Demokratie erst, wenn sie sich nicht nur an bestimmte rechtsförmige Verfahren hält, sondern sich auch zu einer vorstaatlichen, über dem Gesetz stehenden, „überpositiven" Wertordnung bekennt, die zum Beispiel die Wahrung der Menschenrechte als Grundrechte garantiert. Grundrechte sind Persönlichkeitsrechte, die als Freiheits-, Gleichheits- und Unverletzlichkeitsrechte den Einzelnen vor Übergriffen des Staates schützen. Aufgrund der historischen Erfahrung mit der nationalsozialistischen Gewaltherrschaft genießen die Grundrechte im Grundgesetz der Bundesrepublik Deutschland einen besonderen Rang. Als überpositives Recht kann der Staat die Grundrechte nicht gewähren, sondern nur gewährleisten.[7]

Die Hürden, die das Grundgesetz zum Schutz der Grundrechte errichtet hat, sind sehr hoch. Dies gilt für alle Grundrechte und Grundfreiheiten, von der Freiheit der Person, der Gleichheit vor dem Gesetz, der Glaubens-, Meinungs- und Informationsfreiheit, der Versammlungs- und Vereinigungsfreiheit, über die Berufsfreiheit, Freizügigkeit bis zur Unverletzlichkeit der Wohnung und des Brief-, Post- und Fernmeldegeheimnisses, wie in Artikel 10 klar und unmissverständlich formuliert ist: „Das

3 GG, Art. 79, Abs. 3.

4 GG, Art. 19, Abs. 2.

5 GG, Art. 19, Abs. 4.

6 GG, Art. 18.

7 Josef Foschepoth, Staatsschutz und Grundrechte in der Adenauerzeit, in: Jens Niederhut / Uwe Zuber (Hrsg.), Geheimschutz transparent? Verschlusssachen in staatlichen Archiven, Essen 2010, S. 27-58, hier bes. S. 31 ff.: „Grundrechte und Staatsschutz im Grundgesetz".

Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden."[8]

Auch das allgemeine Recht, wie das Postrecht und das Strafrecht, zumindest in seinen frühen Fassungen, spricht eine eindeutige Sprache. Eingriffe in das Post- und Fernmeldegeheimnis sind streng verboten. Laut Postgesetz durften Briefe und sonstige Postsendungen weder geöffnet, noch gelesen oder deren Inhalt an Dritte mitgeteilt werden. Annahme und Beförderung von Postsendungen konnten nicht verweigert werden. Die Post hatte im Gegenteil eine Beförderungspflicht.[9] Nicht zustellbare und verweigerte Sendungen mussten laut Postordnung an den Absender zurückgeschickt werden. Eine Beschlagnahme durfte und darf nur vom Richter verfügt werden.[10] Bei Eingriffen in das Post- und Fernmeldegeheimnis drohte das Strafrecht harte Strafen an. Postbeamte, die sich eines solchen Vergehens schuldig machten, oder deren Vorgesetzte, die dies duldeten oder nicht dagegen vorgingen, konnten „mit Gefängnis nicht unter drei Monaten bestraft"[11] werden.

Soweit die verfassungsrechtlichen und gesetzlichen Normen zur Unverletzlichkeit des Post- und Fernmeldegeheimnis. Angesichts dieser eindeutigen Rechtslage konnte es zumindest in der frühen Bundesrepublik weder Post-, noch Telefonüberwachung gegeben haben, es sei denn, ein allgemeines Gesetz hätte, wie vom Grundgesetz gefordert, entsprechende Beschränkungen definiert. Ein solches Gesetz wurde jedoch erst 1968 vom Deutschen Bundestag verabschiedet. Dann dürfte es zumindest vor 1968 keine Einschränkungen und Verletzungen des Post- und Telefongeheimnisses gegeben haben. Aber auch das war nicht der Fall. Im Gegenteil: Seit Gründung der Bundesrepublik Deutschland wurden seitens des Staates jährlich Millionen von Postsendungen aufgebrochen, beschlagnahmt oder vernichtet und ebenso viele Telefone abgehört, Fernschreiben und Telegramme abgeschrieben, und zwar von den ehemaligen Besatzungsmächten ebenso wie von den Westdeutschen selbst.

---

8 GG, Art. 10, Abs. 1 und 2.

9 Postgesetz (PG), § 3, Abs.1 lautet: „Die Annahme und Beförderung von Postsendungen darf von der Post nicht verweigert werden."

10 Strafprozessordnung (StPO), § 100, Abs. 1.

11 Strafgesetzbuch (StGB), §§ 354, 357-359.

Die Überwachung durch die drei Westmächte

Von der Verfassung nun zur Verfassungswirklichkeit: Bei ihrer Gründung stand die Bundesrepublik Deutschland unter zweierlei Recht, unter dem Grundgesetz, das jeden Eingriff in das Post- und Fernmeldegeheimnis untersagte, und unter dem Besatzungsrecht, das den Besatzungsmächten freie Hand ließ, den gesamten Post- und Fernmeldeverkehr im Westen Deutschlands zu überwachen.

„Schutz der Sicherheit der alliierten Streitkräfte" war die Formel, mit der die westlichen Siegermächte den Aufbau eines umfangreichen Überwachungs- und Geheimdienstapparates im westlichen Teil Deutschlands begründeten. Es war die Formel, die vom Beginn der Besatzungszeit an in allen sicherheitsrelevanten Gesetzen und Verordnungen der drei Besatzungsmächte auftauchte und über das Besatzungsstatut, den Deutschland- und Truppenvertrag, das Zusatzabkommen zum NATO-Truppenstatut bis zu zahlreichen deutsch-alliierten, offenen und geheimen Vereinbarungen immer wieder fortgeschrieben wurde. Es war die Formel, mit der Art und Ausmaß alliierten Handelns in der Bundesrepublik begründet und vor der Öffentlichkeit, dem Parlament oder den Gerichten verschleiert werden konnte.

Die Post- und Fernmeldeüberwachung der Besatzungsmächte erforderte einen großen Kontrollapparat. Allein in Düsseldorf waren in der britischen Überwachungsstelle 90 Leute beschäftigt. Die deutschen Behörden waren angewiesen, aktiv mitzuwirken, ihr Wissen aber geheim zu halten. In den westdeutschen Post- und Fernmeldeämtern von Kiel bis München, von Kaiserslautern bis Hof wurden alliierte Überwachungsstellen eingerichtet, deren Mietverträge erst 1968 endeten, als den westdeutschen Geheimdiensten per Gesetz die Durchführung der Post- und Fernmeldekontrolle übertragen wurde, auch auf Antrag der Alliierten. Natürlich wurden die Alliierten auch danach zum Schutz der Sicherheit der eigenen Truppen selbst tätig.

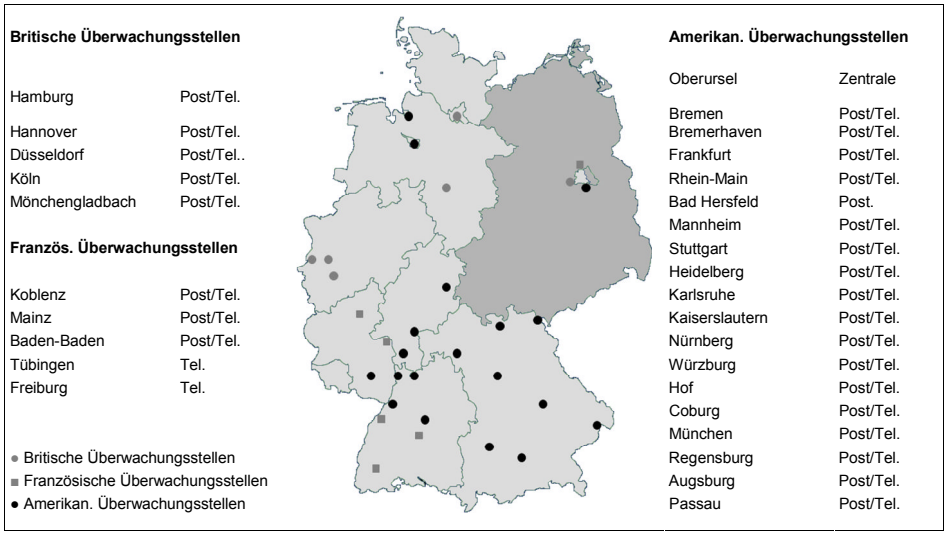


Abb. 1: Alliierte Überwachungsstellen in der BRD, 1949-1968.[12]

Überwacht wurde alles, was von der Bundespost transportiert bzw. übermittelt wurde: Drucksachen, Zeitungen, Briefe, Päckchen und Pakete ebenso wie Telefonate, Fernschreiben und Telegramme. Zunächst waren es die Franzosen, die im Inland „am schärfsten“ [13] überwachten. Den Zensoren mussten alle ein- und abgehenden Postsendungen vorgelegt werden. Auch Bonn wurde überwacht, mithin die gesamte Korrespondenz der Bundesregierung und der Bundestagsabgeordneten. Überwacht wurden ferner sämtliche Telegramme und Telefonanschlüsse. „Ich weiß“, schrieb Heinrich von Brentano, Vorsitzender der CDU/CSU-Fraktion im Deutschen Bundestag, an Bundeskanzler Adenauer, „dass beispielsweise in Mainz die Landesregierung, der Landtag, die Gerichtsbehörden, die politischen Parteien, die konfessionellen Verbände, der Bauernverband, das Regierungspräsidium, die Verlage, die Bischöfliche Kanzlei, der Bischof selbst, eine Anzahl von Anwälten, Landtags- und Bundestagsabgeordnete, bestimmte Firmen und Zeitungen usw. dieser ständigen Kontrolle unterliegen.“[14]

12 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 61.

13 Politisches Archiv des Auswärtigen Amtes (PA AA), B 10/1847, Bundesministerium für das Post- und Fernmeldewesen (BMPF) an Bundeskanzleramt (BKamt), 01.03.1951.

14 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 19, S. 301 f.

Auch die Briten praktizierten zunächst eine exzessive Überwachung. 1953 waren 284 Telefonkabel in der britischen Besatzungszone auf Überwachung geschaltet. In einem Schreiben des Bundespostministeriums an die britische Besatzungsmacht hieß es: „In Düsseldorf sind nach den Unterlagen meiner Postdienste 51 Fernsprechleitungen des öffentlichen Durchgangsverkehrs, darunter 41 öffentliche Auslandsleitungen nach Holland, Belgien, Luxemburg, Frankreich und der Schweiz - 14 Telegraphenleitungen - 9 Fernschreibverbindungsleitungen (sämtliche westliches Ausland) auf Überwachung geschaltet; in Hamburg sind 90 öffentliche Fernsprechleitungen, darunter 53 nach dem westlichen Ausland und den Nordstaaten - 13 Telegraphenleitungen - 6 Fernschreibverbindungsleitungen nach dem westlichen Ausland sowie 18 internationale Durchgangs-Telegraphenleitungen auf Überwachung geschaltet; in Hannover sind über 100 Fernsprechleitungen des öffentlichen Fernsprechverkehrs mit dem In- und Ausland auf Überwachung geschaltet; in Köln sind 43 Fernsprechleitungen - 6 erst vor kurzem neu - und 7 Leitungen nach Berlin auf Überwachung geschaltet."[15] Auch wichtige internationale Durchgangsleitungen wie Brüssel – Wien, Brüssel – Prag, Antwerpen – Wien und Antwerpen – Prag wurden regelmäßig abgehört.[16] Über diese Leitungen ging der wesentliche, wenn nicht der gesamte Telefonverkehr der Bundesrepublik Deutschland mit dem westlichen und dem nördlichen Europa. „Bei dieser Art und diesem Umfang der Abhörmöglichkeit", so das Resümee des Bundesministeriums für das Post- und Fernmeldewesen, „ist ein bedeutender Teil des gesamten politischen und wirtschaftlichen Lebens der Bundesrepublik der alliierten Überwachung ausgesetzt."[17]

Das Interesse der Amerikaner richtete sich weniger auf Einzelüberwachungen als auf strategisch ausgerichtete, flächendeckende Überwachungen in der Bundesrepublik Deutschland. Entlang einer Frontlinie von Norwegen bis Nordafrika wurde ein eigenes Nachrichten- und Überwachungssystem aufgebaut, in dem die Bundesrepublik der strategisch bedeutsamste Teilabschnitt war.[18] Neben der Überwachung des sowjetischen

15 Ebenda, Dok. Nr. 20, S. 303 f.

16 PA AA, B 130/3195, BMPF an Auswärtiges Amt (AA), 18.06.1953.

17 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 20, S. 303.

18 Bayerisches Hauptstaatsarchiv (BayHStA), StK Ministerratsprotokolle 39, Nr. 85, 28.05.1956. „Ministerpräsident Dr. Hoegner teilt mit, die US-Streitkräfte hätten am 27.02.1956 einen Antrag auf Inanspruchnahme eines Geländes auf dem Gipfel des Gro-

Macht- und Einflussbereichs standen auch Länder wie China, Jugoslawien und Kuba auf der Wunschliste der Amerikaner, später auch Indien, Indonesien, Kambodscha, Pakistan, Nordvietnam und Nordkorea. Auch in diesen Fällen wurde der Überwachungsgrund mit dem ‚Schutz der Sicherheit der alliierten Truppen in der Bundesrepublik' angegeben[19]. Im Unterschied zu Briten und Franzosen gelang es der Bundesregierung nicht, die Amerikaner zu einer Vereinbarung zu bewegen, die die individuelle Überwachung auf verdächtige Personen und die allgemeine Überwachung auf die DDR und die übrigen Ostblockstaaten beschränkte.[20]

Individuelle Überwachung	**Überwachte Einzelanschlüsse**
Ehem. Brit. u. Franz. Besatzungszone	51
Ehem. Amerikanische Besatzungszone	286
insgesamt	**337**
Allgemeine Überwachung	**Überwachte Leitungen**
Ehem. Brit. u. Franz. Besatzungszone	2
Ehem. Amerikanische Besatzungszone	175
davon:	
- Leitungen in der BRD	10
- Leitungen von/in die DDR	12
- Leitungen von/ins östliche Ausland	50
- Leitungen von/ins westliche Ausland	41
- Durchgangsleitungen West-Ost/Ost-West	62
Insgesamt	**177**
davon 63 Telefonleitungen, 111 Fernschreibleitungen und 3 Telegraphenleitungen	

Abb. 2: Alliierte Überwachung des Fernmeldeverkehrs in der Bundesrepublik Deutschland, Stand 1.2.1958.[21]

ßen Arbers zur Errichtung einer Nachrichtenstelle gestellt. Durch diese Nachrichtenstelle solle eine Lücke in einer von Norwegen bis Afrika reichenden Kette von Nachrichtenstationen geschlossen werden."

19 PA AA, B 130/5701, Vermerke vom 09.07.1965 und 20.07.1965.

20 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 17.

21 Ebenda, S. 53.

Die Tabelle macht deutlich, dass die Einzelüberwachung, etwa zur Enttarnung von Spionen, Verbindungsleuten oder sonstigen verdächtigen Personen eine deutlich geringere Bedeutung hatte als die allgemeine oder strategische Überwachung. Allgemeine Überwachung bedeutete, dass ganze Telefon-, Fernschreib- oder auch Telegraphenleitungen rund um die Uhr auf Überwachung gestellt und die jeweiligen Gespräche, Fernschreiben und Telegramme aufgezeichnet werden konnten. Auffallend ist der hohe Anteil von überwachten Fernschreibleitungen, wovon 10 Leitungen innerhalb der Bundesrepublik, 41 Leitungen ins westliche Ausland und 37 Leitungen von West- nach Osteuropa verliefen. Lediglich 3 Fernschreibleitungen gingen in die DDR und 23 Leitungen in die übrigen Ostblockstaaten. Hinsichtlich der Telegrafen- und Fernschreibleitungen ist quellenmäßig belegt, dass „von den Amerikanern sämtliche Telegramme und Fernschreiben auf den im amerikanischen Gebiet der Bundesrepublik gelegenen Hauptleitungen mitgeschrieben und die geschlossenen Zweitrollen nach Amerika zur Auswertung gesandt“[22] wurden.

Deutlich wird, dass wir es bei der Überwachung des Fernmeldeverkehrs (Telefonate, Fernschreiben, Telegrammen etc.) in der Bundesrepublik Deutschland durch die Besatzungsmächte, respektive die USA, mit einer Überwachung großen Ausmaßes zu tun haben. Zu bedenken bleibt, dass sich die aktenmäßig belegten Zahlen nur auf den drahtgebundenen Weg des Fernmeldeverkehrs über die deutschen Postämter beziehen. Unberücksichtigt bleibt die quantitativ nicht belegte drahtlos, über Funk vermittelte Telekommunikation, die durch Richtfunkantennen jederzeit abgehört werden konnte, ohne dass es dazu eines Partners wie der Deutschen Bundespost bedurfte. Dies geschah über die verschiedenen Militärbasen und Abhörstationen der Amerikaner in Berlin und entlang der innerdeutschen Grenze, nicht zuletzt über den Fernsprechknotenpunkt in Frankfurt, wo „die meisten Richtleitungsnetze der Post“ zusammenkamen und von den Amerikanern abgehört wurden.[23]

Nicht weniger exzessiv als die Überwachung des Fernmeldeverkehrs war die Überwachung des Postverkehrs durch die USA. Auch hier ging es um strategische Überwachung. Millionenfach wurden Briefe aus dem Verkehr gezogen, geöffnet, ausgewertet und danach wieder in den Post-

22 Bundesarchiv (BArch), B 106/200007, Überwachung des Post- und Fernmeldeverkehrs durch die Drei Mächte, 05.03.1958, S. 6.

23 Klaus Beyrer (Hrsg.), Streng geheim. Die Welt der verschlüsselten Kommunikation, Frankfurt 1999, S. 154 und 166.

verkehr zurückgegeben. Exakte Zahlen liegen nicht vor, jedoch pauschalierte Berechnungen und Schätzungen, immerhin von amtlicher Seite. Aus Abrechnungen der Deutschen Bundespost für die den Amerikanern hierfür in den Jahren 1960 bis 1967 erbrachten Leistungen konnten Zahlen ermittelt werden, die erneut den großen Umfang auch der strategischen Postüberwachung der Amerikaner in der Bundesrepublik deutlich machen.

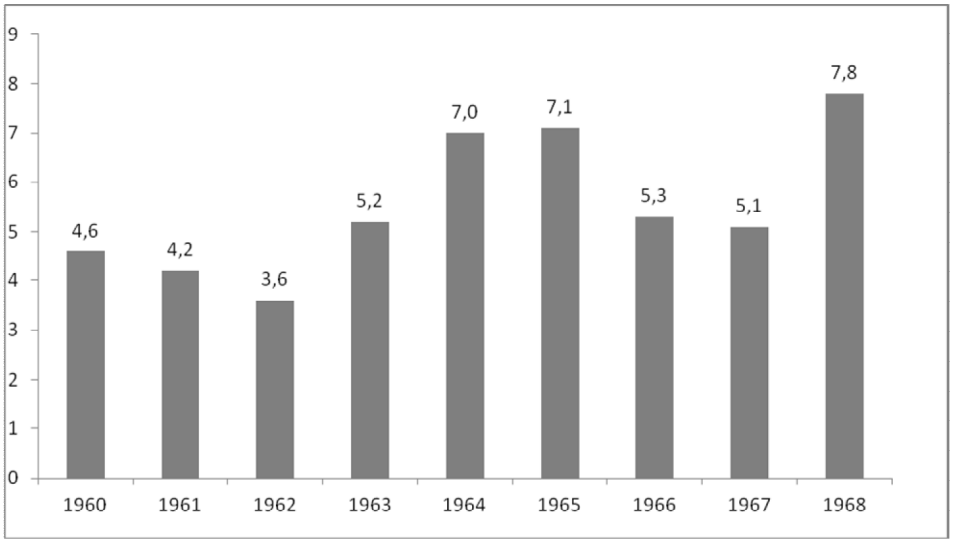


Abb. 3: Amerikanische Postüberwachung in der Bundesrepublik Deutschland, 1960-1968.[24]

Da die amerikanischen Stellen, wie es 1960 hieß[25], die Kontrolle der Postsendungen im Wesentlichen in dem früheren Umfang beibehielten, ist davon auszugehen, dass die ermittelten Werte für die gesamten Fünfziger- und Sechzigerjahre repräsentativ sind. Im Durchschnitt musste die Deutsche Bundespost den Amerikanern jährlich zwischen fünf und sieben Millionen Postsendungen zu geheimdienstlicher Kontrolle und Auswertung vorlegen. Entsprechendes dürfte für den Umfang der Einzelüberwachungsmaßnahmen gelten. Für 1955 heißt es, dass „die Zahl der Einzelpostüberwachung in der amerikanischen Zone 1 320“ im Jahr betrage,

24 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 56.

25 BArch, B 106/200007, Konsultationsbesprechungen mit den USA, 21.03.1960.

wobei zu berücksichtigen sei, „dass zum Zwecke der Tarnung nicht die Post des einzelnen Empfängers, sondern die Post für jeweils zwei bis drei Häuser zur Vorlage kommen muss“[26]. Anfang 1958 waren es 2 077 Einzelpersonen und 173 Häusergruppen, deren Post von den Amerikanern in Einzelüberwachung zensiert wurde. Allein 212 Postämter wurden für die Durchführung dieser Maßnahme benötigt.[27] Bemühungen, die amerikanischen Behörden zu bewegen, wenigstens in Sachen Postverkehr die Überwachungen zu reduzieren, scheiterten ebenfalls, was den Deutschen „große Sorgen“[28] machte.

Die Überwachung durch die Westdeutschen

Die Westdeutschen waren jedoch keineswegs nur Betroffene einer harten Überwachungspraxis der Besatzungsmächte, sondern wurden auch selbst aktiv, als sich zu Beginn der Fünfzigerjahre der Propagandakrieg zwischen beiden deutschen Staaten verschärfte. 1951 wurde das politische Strafrecht, das die Siegermächte 1945 erst abgeschafft hatten, wieder eingeführt und verschärft. Danach musste jede politische Handlung, die als „staatsgefährdend“ eingeschätzt wurde, strafrechtlich verfolgt werden. Hierzu zählten auch die Einfuhr und Verbreitung „verfassungsverräterischer“ oder „staatsgefährdender“ Schriften und Materialien.[29] Diese kamen in der Regel aus der DDR, wurden aber auch in der Bundesrepublik Deutschland auf die Post gegeben.

Mit großer Perfektion entwickelten nun die Westdeutschen eine spezielle Form der Überwachung, die den gesamten Postverkehr mit der DDR betraf. Die Aufgabe übernahmen nicht etwa die Geheimdienste, sondern die ganz normalen Beamten, die Post- und Zollbeamten, die Staatsanwälte und Richter in den grenznahen Gebieten. Ein gegliedertes System zentraler und dezentraler Aussonderungsstellen erfasste im Laufe

26 PA AA, B 130/5535, BMPF an Bundeskanzler Adenauer, 06.06.1955.

27 PA AA, B 130/5535, BMPF an AA, Gesamtzusammenstellung der Überwachung, 04.03.1958.

28 PA AA, B 130/5535, Überwachung des Post- und Fernmeldeverkehrs durch die Drei Mächte, 07.01.1957, S. 2.

29 Vgl. Reinhard Schiffers, Zwischen Bürgerfreiheit und Staatsschutz. Wiederherstellung und Neufassung des politischen Strafrechts in der Bundesrepublik Deutschland 1949-1951, Düsseldorf 1989, bes. S. 347-361.

der Zeit etwa 80 Prozent der eingehenden Post aus der DDR.[30] Seit 1951 gab es in Hannover eine „zentrale Aussonderungsstelle". Weitere Zentralstellen wurden in Hamburg, Bad Hersfeld und Hof eingerichtet. Die beschlagnahmte Post belief sich laut Monats- und Jahresberichten des Bundesamtes für Verfassungsschutz allein in den Jahren 1955 bis 1968 auf 100 Millionen Sendungen.[31]

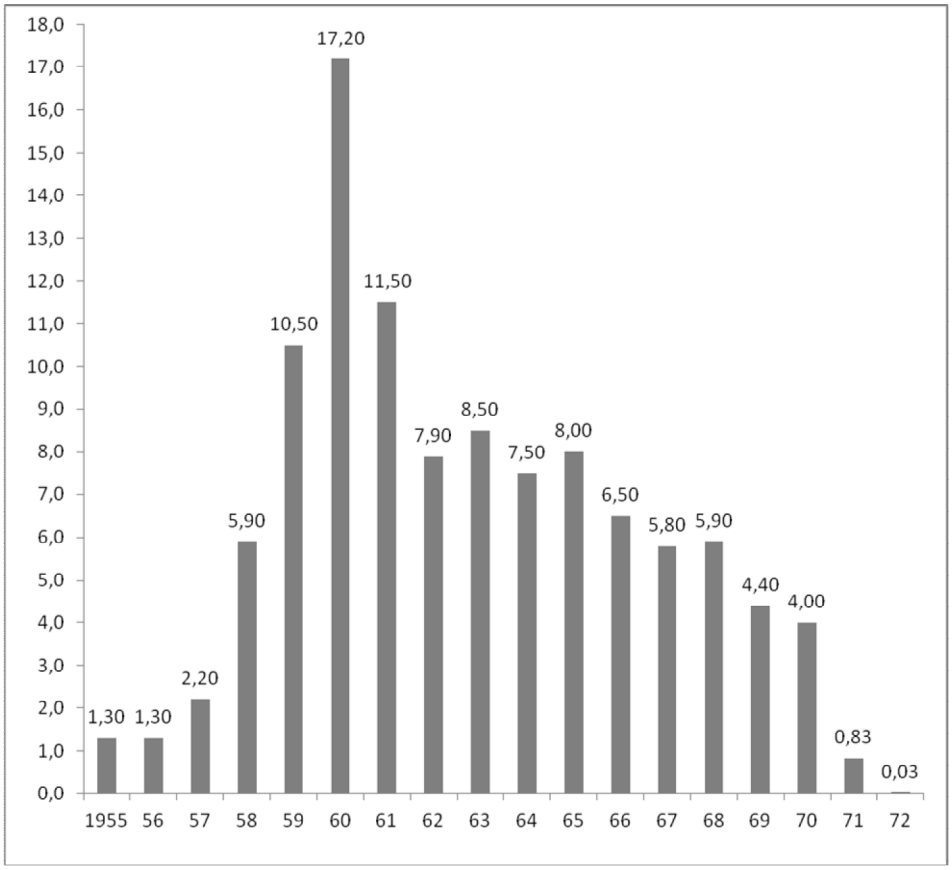


Abb. 4: Beschlagnahmte Postsendungen aus der DDR, 1955 -1972.[32]

30 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 115.

31 BArch, B 443/529, B 443/531, B 137/16514, B 443/559.

32 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 116.

Die Durchsuchung der Post aus der DDR begann bereits an der Zonengrenze. Postbeamte bestiegen die Postzüge und sortierten verdächtige Sendungen aus. Bei Verdacht auf staatsgefährdendes Material reichten sie die Sendungen an den Zoll, die Sendungen aus dem Inland sofort an die Staatsanwaltschaft weiter. Der Staatsanwalt leitete daraufhin pro forma ein Strafverfahren ein, um einen richterlichen Beschlagnahme-Beschluss zu erwirken. Danach stellte er das Verfahren ein. Von den beschlagnahmten Sendungen wurde der größte Teil vernichtet, der Rest als Beweismaterial für Ermittlungs- und Strafverfahren genutzt. So landeten nicht nur „staatsgefährdende Briefe", sondern auch mancher „liebe Brief" aus Ostberlin und der DDR statt beim Adressaten im Gefängnis von Hannover. Hier stand ein Reißwolf, in dem Strafgefangene die beschlagnahmten Postsendungen vernichten mussten.[33]

Angesichts der Fülle der beschlagnahmten Briefe und Postsendungen verlief die staatliche Postüberwachung keineswegs geräuschlos. Einige beschwerten sich oder reichten Klage ein, in der Regel vergeblich. Wissenschaftler erhielten die abonnierten Zeitschriften aus Osteuropa nicht mehr und protestierten. Abgeordnete vermissten ihre Briefe, Zeitungen und sonstigen Informationen aus der DDR. „Tatsächlich", so der SPD-Bundestagsabgeordnete Adolf Arndt in einem Brief vom 4. Januar 1956 an den bayerischen Staatsminister der Justiz, „üben die Postbehörden im Zusammenwirken mit den Staatsanwaltschaften und den Amtsgerichten eine verfassungswidrige Zensur aus"[34].

Das praktizierte Verfahren zur Überwachung des Postverkehrs mit der DDR war rechtsstaatlich höchst bedenklich, da die Beschlagnahme nicht der Beweiserhebung und Einleitung eines Gerichtsverfahrens diente, sondern lediglich einer wie auch immer zu bewertenden „Gefahrenabwehr". „Es ist der Gerichte nicht recht würdig", beschwerte sich Amtsgerichtspräsident Heim von Hannover auf dem Dienstweg, „in ein solches Verfahren eingeschaltet zu sein, zumal das , was sie hier verrichten sollen, im Grunde mit Rechtspflege nichts mehr zu tun hat".[35]

Eine grundgesetzkonforme Beschränkung des Postgeheimnisses hat es – soweit es die Überwachung des Postverkehrs mit der DDR anbetrifft – nicht gegeben. Auch 1968, als erstmals ein Gesetz zur Überwachung des

33 Der Spiegel, Nr. 34, 1964, S. 26.

34 BArch, B 141/17358.

35 BArch, B 141/3837, Schreiben an den Oberlandesgerichtspräsidenten in Celle, 14.4.1955.

Post- und Fernmeldeverkehrs zu nachrichtendienstlichen Zwecken verabschiedet wurde, galt dies nicht für den innerdeutschen Postverkehr. Hier blieben weiterhin die Post- und Zollbeamten, die Staatsanwälte und Richter zuständig. Alles, was dem Anschein nach Waren enthielt – das konnten auch Briefe von 20 Gramm sein – hatten die Postbeamten ihren Kollegen vom Zoll vorzulegen. Nur der Zoll durfte die verschlossenen Sendungen öffnen. Wurde dabei „Staatsgefährdendes" gefunden, wozu zum Beispiel auch die mehrbändige Geschichte der Arbeiterbewegung gehörte, konnte dies vom Staatsanwalt konfisziert oder ein entsprechendes Strafverfahren eingeleitet werden, wie das „Gesetz zur Überwachung strafrechtlicher und anderer Verbringungsverbote" von 1961 bestimmte.[36]

Ein allgemeines Gesetz zur Einschränkung des Post- und Fernmeldegeheimnisses schien bis 1968 politisch nicht durchsetzbar zu sein. Weder in Bundestag und Bundesrat, noch in der Öffentlichkeit war mit einer mehrheitlichen Unterstützung für ein Zensurgesetz zu rechnen. Möglich schien allenfalls ein Gesetz mit hohen restriktiven Auflagen, was wiederum von der Exekutive nicht gewollt war. Es konnte den Kampf des Staates gegen den Kommunismus nur erschweren. So versuchte die Administration seit Beginn der Fünfzigerjahre durch Anweisungen, Verordnungen, Rechtsgutachten und Einzelregelungen, versteckt in verschiedenen Gesetzen gleichsam um das Grundgesetz herum, einen rechtlichen Rahmen zu zimmern, der das Handeln der Exekutive absichern und legitimieren sollte.

Nach und nach entstand ein juristisches Konstrukt, das im Wesentlichen auf folgenden politischen und rechtlichen Überlegungen basierte:

1. Besatzungsrecht: Angesichts der eindeutigen Gesetzeslage war der Kampf gegen die Verbreitung kommunistischer Propaganda auf dem Postwege nur im Geheimen, ohne Öffentlichkeit und parlamentarische Kontrolle zu führen. Dazu bot das Besatzungsrecht, das über dem Grundgesetz stand, den willkommenen Rahmen.[37]

---

36 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 33, S. 319.

37 BArch, B 141/17360. Die Teilung Deutschlands sei von den Besatzungsmächten herbeigeführt worden, so die etwas sonderbare Argumentation. Deshalb bestünden „keine politischen Bedenken" dagegen, dass ein Besatzungsgesetz „zur Grundlage von Eingriffen in Grundrechte, insbesondere Art. 10 GG, gemacht wird". Bundesminister für Wirtschaft an Bundesminister für Justiz (BMJ), 23.4.1957.

2. Verfassungsrecht: Um den Staatsschutz als vorrangig definieren und die Grundrechte als unmittelbar geltendes Recht relativieren zu können, wurde der „Grundsatz der Güterabwägung" auch in das Verfassungsrecht eingeführt. Der Schutz der Grundrechte setzte nach Ansicht des Bundesjustizministeriums den Schutz des Staates als „höherwertiges Gut" voraus.[38]

3. Strafrecht: Mit der Wiedereinführung des politischen Strafrechts Anfang der Fünfzigerjahre wurden Herstellung, Vervielfältigung, Verbreitung und Einfuhr hochverräterischen oder staatsgefährdenden Propagandamaterials unter Strafe gestellt. Da gleichzeitig das Legalitätsprinzip, der strafrechtliche Verfolgungszwang auch für politische Straftaten, eingeführt wurde, war der Staatsanwalt gezwungen, „staatsgefährdende Schriften" strafrechtlich zu verfolgen.[39]

4. Zollrecht: Nach der „Interzonenhandelsüberwachungsverordnung" von 1951 waren sämtliche Postsendungen aus der DDR dem Zoll vorzuführen, sofern sie dem Anschein nach Waren enthielten. Auch Bücher, Broschüren, Zeitungen wurden jetzt als Waren definiert. Stießen die Zollbeamten bei der Suche nach Handelsware „zufällig" auf Propagandamaterialien, waren diese dem Staatsanwalt zu übergeben.[40]

5. Beamtenrecht: Das wichtigste Glied in der Kette war der Beamte, der die eigentliche Zensur ausübte. Aus Treuepflicht dem Staat gegenüber war er gehalten, jede mögliche strafbare Handlung abzuwenden und dem Vorgesetzten Mitteilung zu machen. Dieser hatte unverzüglich Anzeige zu erstatten. Die Treuepflicht wurde zur Anzeigenpflicht und damit zum wichtigsten Instrument einer grundgesetzwidrigen Postzensur und Telefonüberwachung.[41]

---

38 BArch, B 141/3834, Rechtsgutachten des BMJ über die postalische Behandlung staatsfeindlicher Schriften vom 2.4.1952.

39 StGB, § 93. Danach wurden Einfuhr und Verbreitung staatsgefährdender „Schriften, Schallaufnahmen, Abbildungen oder Darstellungen" mit Gefängnis bestraft. Schon der Versuch war strafbar.

40 BArch, B 106/16106, 27.11.1951.

41 BArch, B 106/16106, 11.6.1952. Das Bundesjustizministerium vertrat die Auffassung, „dass der Staatsschutz vornehmste Aufgabe jedes Beamten sei. Die Verpflichtung zur Treue gegen den Staat zwänge ihn bei jedem Bekanntwerden von staatsfeindlichen Angriffen, z. B. in der Form von Propagandaschriften zur Meldung an die Staatsanwaltschaft. Beamte, die das nicht täten, verstießen gegen die Dienstpflichten und könnten disziplinarisch belangt werden."

Neben der speziellen Überwachung des innerdeutschen Postverkehrs waren auch die nach und nach professioneller werdenden Geheimdienste, Verfassungsschutz und Bundesnachrichtendienst, auf dem Gebiet der Überwachung des Post- und Fernmeldeverkehrs in der Bundesrepublik Deutschland tätig. Hier arbeiteten sie eng mit den Besatzungsmächten und späteren Alliierten eng zusammen. Täglich erhielten Verfassungsschutz und Bundesnachrichtendienst von den amerikanischen und britischen Geheimdiensten Informationen und Lageberichte, die aus der Post- und Fernmeldeüberwachung gewonnen worden waren.

Aus Berlin wurde berichtet, „dass die Verfassungsschutzämter zwar beachteten, dass ihnen selbst das Abhören von Telefongesprächen verboten sei, dass sie aber die amerikanische Dienststelle benutzen würden, um über sie Mitteilungen über Ferngespräche, die für den Verfassungsschutz einschlägig seien, zu erhalten".[42] Auch die Frage, „ob die von britischer Seite bei der Überwachung des Post- und Fernmeldeverkehrs mit den Ostblockstaaten gewonnenen Erkenntnisse auch den dafür zuständigen deutschen Stellen zugänglich gemacht werden", wurde in einem internen Vermerk des Auswärtigen Amtes dahingehend beantwortet, „dass das geschieht".[43]

Die enge Zusammenarbeit und der intensive Daten- und Informationsaustausch zwischen den alliierten und westdeutschen Geheimdiensten waren nicht nur gängige Praxis, sondern wurden auch von beiden Seiten gewünscht und immer wieder vertraglich eingefordert und bestätigt. Die Notwendigkeit der Zusammenarbeit wurde mit dem Schutz der alliierten Truppen begründet und erstreckte sich „namentlich auf die Sammlung, den Austausch und den Schutz aller Nachrichten, die für diese Zwecke von Bedeutung sind".[44] So entstand im Laufe der Zeit ein großer deutsch-alliierter nachrichtendienstlicher Komplex. Wie eng die Zusammenarbeit war, lässt schon eine Stellungnahme des Bundesamtes für Verfassungsschutz aus dem Jahre 1963 erahnen. Darin heißt es: „Die Nachrichtendienste der verbündeten Staaten lassen sich in den die gemeinsame Sicherheit betreffenden Angelegenheiten nahezu als einheitlicher

42 BArch, B 106/200006, Staatssekretär Ritter von Lex an Bundesinnenminister Gerhard Schröder, 21.9.1956.

43 PA AA, B 130/5535, Vermerk Oncken, 3.6.1957.

44 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 8, Zusatzabkommen zum NATO-Truppenstatut, Art. 3, Abs. 2., S. 284.

nachrichtendienstlicher Organismus kennzeichnen; daher die gegenseitige Verpflichtung zum umfassenden Informationsaustausch."[45]

Vom Besatzungsrecht zum Vorbehaltsrecht der Alliierten

Im Frühjahr 1952 verhandelten die Vertreter der Drei Mächte und der Bundesrepublik Deutschland erstmals über die Ablösung des Besatzungsregimes. Ein Konvolut von Verträgen wurde erstellt und verhandelt. Die Verhandlungen über die sog. Westverträge konnten aufgrund der Ablehnung Frankeichs erst in einem zweiten Anlauf im Herbst 1954 zu einem erfolgreichen Abschluss geführt werden. Nach erfolgter Ratifizierung traten sie am 5. Mai 1955 in Kraft. In den Verhandlungen spielte die Frage der Überwachung des Post- und Fernmeldeverkehrs in der Bundesrepublik eine wichtige Rolle. Die Besatzungsmächte drängten auf eine gesetzliche Regelung, die es den alliierten Streitkräften auch nach dem Ende der Besatzungszeit ermöglichten, allgemeine Überwachungsmaßnahmen durchzuführen. „Die Streitkräfte hier in Deutschland", so der britische Hochkommissar Hoyer Millar an Bundeskanzler Konrad Adenauer, „legen großen Wert auf die Überwachung des Nachrichtenverkehrs mit dem Ausland zur Beschaffung von strategischen Informationen sowie auf ein gewisses Maß von Überwachung des Inlandverkehrs aus Gründen der Sicherheit der Streitkräfte."[46]

Um die Forderung der Besatzungsmächte zu erfüllen, war dreierlei erforderlich: 1. die Änderung des Grundgesetzes, 2. die Verabschiedung eines Gesetzes zur Überwachung des Post- und Fernmeldeverkehrs, 3. der Aufbau eines westdeutschen Geheimdienstes, der zur Erledigung einer solchen Aufgabe auch fähig war. Von Anfang an drängten die Westmächte darauf, den Aufbau eines professionellen deutschen Geheimdienstes zu beschleunigen. Bedingung war, dass die deutschen Dienste in der Lage sein würden, sämtliche Formen alliierter Überwachung des Post- und Fernmeldeverkehrs, von der Einzelüberwachung bis zur strategischen Überwachung ganzer Städte, Regionen und Länder zu übernehmen. Dazu waren jedoch zunächst weder das Bundesamt für Verfassungsschutz, noch der Bundesnachrichtendienst, der erst 1956 gegründet wurde, in der Lage.

45 BArch, Nachlass (NL) Brentano, N 1239/83, Der Nachrichtenaustausch zwischen dem Bundesamt für Verfassungsschutz und den alliierten Nachrichtendiensten, 25.9.1963.

46 PA AA, B 130/5701, Hoyer Millar an Adenauer, 29.7.1954.

Außerdem weigerte sich der zuständige Bundesinnenminister Gerhard Schröder, die politische Verantwortung für ein derart weitgehendes Gesetz zu übernehmen. In der Bevölkerung, im Parlament und in der Presse stoße ein solches Gesetz „auf breiteste Ablehnung", schrieb er an Bundeskanzler Adenauer. Allgemein werde erwartet, dass mit der Wiedererlangung der Souveränität die von den Besatzungsmächten ausgeübte Zensur ein Ende finde. Wenn bekannt würde, dass die Bundesregierung auf Druck der früheren Besatzungsmächte, die ausländische Überwachung lediglich durch eine deutsche Überwachung ersetze, würde sich die bisherige Kritik an den Besatzungsmächten künftig gegen die Bundesregierung wenden.[47]

Als Bundeskanzler Adenauer am 19. Oktober 1954 nach Paris fuhr, um mit den Außenministern der Drei Mächte über die Ablösung des Besatzungsregimes zu verhandeln, kam er mit leeren Händen. Ein Gesetz, das die Überwachung des Post- und Fernmeldeverkehrs erlaubte, wie von den Besatzungsmächten gefordert, hatte er nicht im Gepäck. Das hatte zur Folge, dass mit dem Ende der Besatzungsherrschaft alle Überwachungsmaßnahmen eingestellt werden mussten oder nur unter Bruch der Verfassung entweder von den Deutschen allein oder gemeinsam mit den Alliierten fortgeführt werden konnten. Da die Siegermächte in dieser Frage eine besonders unnachgiebige Haltung einnahmen, entstand für den Kanzler eine schwierige Situation. Adenauer ergriff gleich zu Beginn der Beratung über diese Frage die Initiative. Er schlug vor, die drei westlichen Außenminister sollten ihm einen Brief schreiben, in dem sie sich das Recht auf Überwachung des Post- und Fernmeldeverkehrs so lange vorbehalten würden, bis die Bundesregierung aufgrund eines deutschen Gesetzes ermächtigt sei, entsprechende Überwachungsmaßnahmen durchzuführen.

Das, was der Bundeskanzler der Bundesrepublik Deutschland vorschlug, bedeutete nicht weniger als eine schwere Verletzung des Grundgesetzes. Durch diesen Trick sollte das Grundrecht auf Unversehrtheit des Post- und Fernmeldegeheimnisses umgangen werden, um verfassungswidrige Überwachungen durch ein Fortschreiben alliierten Rechts weiterhin zu ermöglichen. Um zu verhindern, dass der Kanzler, der eigentlich alle alliierten Vorbehaltsrechte – mit Ausnahme des Vorbehalts für Berlin und Deutschland als Ganzes – bei den Pariser Verhandlungen abschaffen

47 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 164.

wollte, dafür politisch verantwortlich gemacht wurde, durfte das neue Vorbehaltsrecht auf keinen Fall in den ausgehandelten Vertragstexten stehen. Deshalb bat Adenauer, den Überwachungsvorbehalt in einem separaten Schreiben an ihn zu formulieren. Jedes Wort dieses Schreibens war mit ihm abgestimmt worden. Wie aus den Akten des Auswärtigen Amtes hervorgeht, „ist der Wortlaut des Schreibens vorher mit den Alliierten ausgehandelt worden, da verschiedene Entwürfe nach einander hierfür aufgestellt worden sind".[48]

Über den 5. Mai 1955 hinaus, den der Bundeskanzler zum „Tag der Souveränität"[49] erklärte, behielten die Alliierten somit weiterhin das Recht, Postsendungen zu kontrollieren und Fernmeldeverbindungen zu überwachen. Dieses „bezüglich des Schutzes der Sicherheit der Streitkräfte" vorbehaltene Recht sollte erlöschen, wie es in dem Schreiben der drei Außenminister an Adenauer hieß „sobald die zuständigen deutschen Behörden aufgrund einer deutschen gesetzlichen Regelung in der Lage sind, wirksame Maßnahmen zu ergreifen".[50]

Die Ablösung des neuen alliierten Vorbehaltsrechts, wie die Drei Mächte immer wieder betonten, war an die Beibehaltung bisheriger Überwachungsmöglichkeiten zur Beschaffung geheimdienstlicher Informationen von westdeutschem Boden aus gekoppelt. Die von Adenauer gewünschte Vorgehensweise setzte nicht nur die grundgesetzlich garantierte Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses außer Kraft, sondern auch das Mitwirkungsrecht des Deutschen Bundestags. Die Abgeordneten hatten keine andere Wahl, als sich dem einseitig erklärten Überwachungsvorbehalt der Alliierten zu unterwerfen und eines Tages ein den Vorstellungen der Westmächte entsprechendes deutsches Gesetz zur Ablösung des alliierten Vorbehaltsrechts zu verabschieden, wie es dann tatsächlich 1968 auch geschah. Die von Adenauer erstrebte (beschränkte) Souveränität der Bundesrepublik Deutschland wurde mit einem doppelten Verfassungsbruch erkauft, wie der erst jetzt bekannt gewordene Vorgang über das den Besatzungsmächten bei den Verhand-

48 PA AA, B 130/5701, Auswärtiges Amt an Bundesministerium des Innern, 7.2.1964.

49 Konrad Adenauer, Erinnerungen 1953-1955, Stuttgart 1966, S. 432.

50 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 11b, S. 287.

lungen über die Westverträge 1954 vorbehaltene Recht auf Überwachung zeigt.[51]

Grundgesetzänderung und G 10-Gesetz

1968 ist ein Jahr, das mit tiefgreifenden Veränderungen in Politik und Gesellschaft verbunden ist. Es war das wohl arbeitsintensivste Jahr der Großen Koalition unter Kurt Georg Kiesinger und Willy Brandt. Etliche Reformprojekte wurden auf den Weg gebracht und manche Altlasten der Adenauerzeit beseitigt. Zu letzteren zählten vor allem die Notstandsgesetzgebung, aber auch das Gesetz zur Beschränkung des Post- und Fernmeldegeheimnisses, das sogenannte G 10-Gesetz. Beide Gesetze waren nötig, um die von Adenauer mit den Alliierten ausgehandelten Vorbehaltsrechte, den Notstandsvorbehalt und den Überwachungsvorbehalt abzulösen. Mehr als 13 Jahre waren vergangen, ohne dass die Regierungen Adenauer und Erhard in der Lage gewesen wären, ein rechtsstaatlich einwandfreies Gesetz auf den parlamentarischen Weg zu bringen. 1968 machte sich die Große Koalition mit einer Mehrheit von deutlich mehr als Zwei-Drittel der Abgeordneten ans Werk. Da konnten schon mal 100 Abgeordnete aus den eigenen Reihen dagegen stimmen, ohne die Verabschiedung eines umstrittenen Gesetzes zu gefährden. Die SPD-Führung wollte es wissen und ihre Regierungsfähigkeit unter Beweis stellen.

Das Ergebnis ist bekannt. Nicht nur die Notstandsgesetze, sondern auch das G 10-Gesetz wurde mit großer Mehrheit verabschiedet. „Die Vorbehaltsrechte nach Art. 5, Abs. 2 des Deutschlandvertrages erlöschen endgültig“, erklärte Außenminister Brandt im Deutschen Bundestag. Künftig würden „auf dem Gebiet der Post- und Fernmeldeüberwachung nicht mehr die Alliierten aufgrund des von ihnen vorbehaltenen Besatzungsrechts tätig werden, sondern deutsche Behörden aufgrund der sie bindenden deutschen Gesetze“[52].

Die Ablösung der Vorbehaltsrechte war der politische Schlüssel, mit dem nicht nur die Notstandsgesetze, sondern auch das G 10-Gesetz über die parlamentarischen Hürden gebracht wurden. Mit Erfolg wurde öffentlich der Eindruck vermittelt, als habe es nur den Deutschlandvertrag von 1955 als Rechtsgrundlage für die alliierte Überwachungspraxis gegeben.

51 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 36-48.

52 Ebenda, S. 192.

Dieses Recht sei nun endgültig erloschen. Das G 10-Gesetz konnte so als eine Art Befreiung von den letzten Restriktionen der Besatzungszeit und somit als Souveränitätsgewinn für die Bundesrepublik Deutschland gefeiert werden. Vor allem die SPD, für die die Durchsetzung der Notstandsgesetzgebung und des „Abhörgesetzes" ein wichtiger Ausweis ihrer Regierungsfähigkeit war, äußerte sich gern in diesem Sinne: „Bis 1968 kontrollierten die USA, Großbritannien und Frankreich in der Bundesrepublik Postsendungen und hörten Telefone ab, wie dies Besatzungsmächte in eroberten Ländern zu tun pflegen: Von niemandem kontrolliert und nach eigenem freien Ermessen. Erst als Bundestag und Bundesrat eine eigene deutsche Regelung durch Ergänzung des Grundgesetzes und Schaffung eines besonderen Gesetzes („G 10-Gesetz") getroffen hatten, erloschen die alliierten Befugnisse."[53]

Tatsächlich wurde das Vorbehaltsrecht nach Deutschlandvertrag von 1955 abgelöst. Dort war jedoch nur allgemein von den „bisher innegehabten und ausgeübten Rechten" zum Schutz der Sicherheit der alliierten Truppen die Rede. Ausgeführt wurden sie jedoch in Art. 4 des Truppenvertrags von 1955 und in Art. 3 des Zusatzabkommens zum NATO-Truppenstatut, das den Truppenvertrag 1959 ablöste und bis heute gilt. Darin verpflichteten sich beide Seiten auf enge geheimdienstliche Zusammenarbeit und strikte Geheimhaltung, vor allem auf dem Gebiet der Überwachung, der „Sammlung, den Austausch und den Schutz aller Nachrichten, die für diese Zwecke von Bedeutung sind".[54] Auf das Vorbehaltsrecht nach Deutschlandvertrag konnten die Drei Mächte ruhig verzichten, die unbeschränkte Fortführung der Überwachung war längst durch das Zusatzabkommen zum NATO-Vertrag und einer geheimen Verwaltungsvereinbarung zum G10-Gesetz dauerhaft gesichert. Das erwähnte Willy Brandt in seiner Rede vor dem Deutschen Bundestag jedoch nicht.

In der geheimen Zusatzvereinbarung zum G 10-Gesetz vom 28. Oktober 1968 wurden die Vertragsparteien konkreter. Die Regierungen der Bundesrepublik Deutschland und der Drei Mächte kamen überein, dass die bisher „innegehabten und ausgeübten Rechte (Vorbehaltsrechte) in Bezug auf den Brief-, Post- und Fernmeldeverkehr abgelöst werden, in-

53 BArch, B 257/68699, Sozialdemokratischer Pressedienst vom 11.09.1978, S. 4.

54 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 8, S. 284.

dessen nach Art. 3 Abs. 2 des Zusatzabkommens zum NATO-Truppenstatut vom 3. August 1959 die deutschen Behörden und die Behörden der Stationierungsstreitkräfte verpflichtet bleiben, in gegenseitiger Unterstützung und enger Zusammenarbeit die Sicherheit der Bundesrepublik Deutschland, der Entsendestaaten und ihrer Truppen zu fördern und zu wahren, indem sie insbesondere alle Nachrichten, die für diese Zwecke von Bedeutung sind, sammeln, austauschen und schützen“[55].

Im Klartext bedeutete dies, dass beide Seiten, Deutsche und Alliierte, nach NATO-Recht verpflichtet blieben, auch in Zukunft eng zusammenzuarbeiten, *alle* Nachrichten zum Schutz der Sicherheit der alliierten Truppen zu *sammeln,* also auch weiterhin eigene Überwachungsmaßnahmen durchzuführen, und deren Ergebnisse untereinander auszutauschen. Auch gemeinsame Operationen waren in Zukunft weiterhin möglich. „Soweit es erforderlich werden sollte, dass ein Beauftragter des anregenden Entsendestaates bei der Anwendung einer Beschränkungsmaßnahme anwesend ist, wird das BfV [Bundesamt für Verfassungsschutz] bzw. der BND [Bundesnachrichtendienst] den Zutritt gestatten.“[56] Sogar die Durchführung alliierter Überwachungsmaßnahmen in deutschen Räumlichkeiten sollte beibehalten werden, wie Außenminister Willy Brandt bei Erläuterung des geheimen Zusatzabkommens im Kabinett betonte: „Der deutsche Dienst stellt im Rahmen seiner Befugnisse gemäß dem Gesetz zu Artikel 10 GG seine Kontrollmöglichkeiten beziehungsweise deren Ergebnisse den Amerikanern auf Anforderung zur Verfügung.“[57]

55 PA AA, B 130/5761, Geheime Verwaltungsvereinbarung zum G10 Gesetz, 22.10.1968, Präambel.

56 PA AA, B 130/5761, Geheime Verwaltungsvereinbarung, Art. 4 Abs 4.

57 PA AA, B 86/894, Ergänzender Sprechzettel für die Kabinettssitzung am 22. Mai 1968.

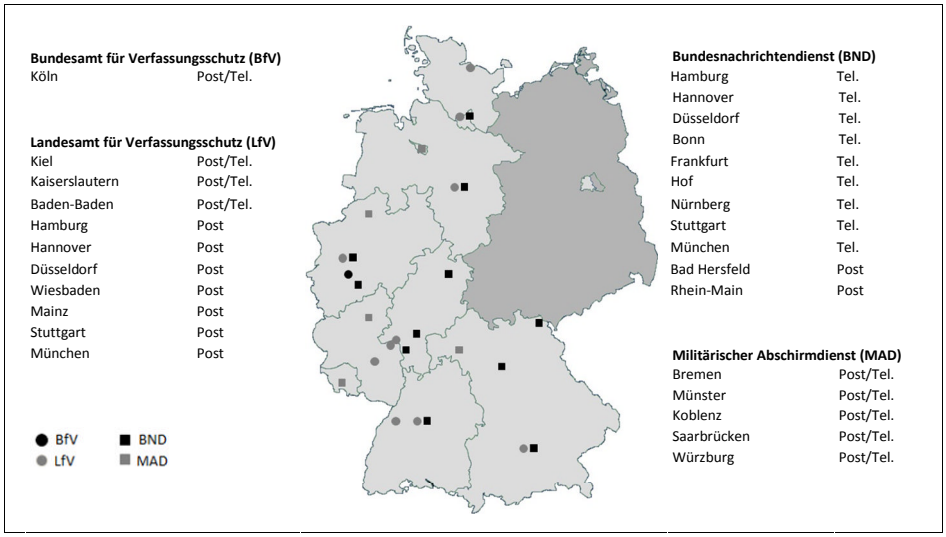


Abb. 5: Überwachungsstellen für Post- und Fernmeldeverkehr der westdeutschen Geheimdienste ab 1968.[58]

Um die Übergabe der Überwachung von den Alliierten auf die Deutschen schnellstmöglich zu regeln, übernahmen die deutschen Nachrichtendienste Räume, Einrichtungsgegenstände, technisches Gerät und teilweise auch Personal von den alliierten, vor allem den amerikanischen Überwachungsstellen.[59] In enger Zusammenarbeit von BfV, LfV (Landesämter für Verfassungsschutz), BND und MAD (Militärischer Abschirmdienst) wurde in kurzer Zeit ein Verbundsystem aufgebaut, das eine effiziente und flächendeckende Kontrolle des Post- und Fernmeldeverkehrs in der gesamten Bundesrepublik Deutschland ermöglichen sollte. Dieses System mit 20 bis 25 zentralen Überwachungsstellen war so üppig ausgestattet, damit es nicht nur individuelle, sondern auch allgemeine oder strategische Überwachungsmaßnahmen durchführen konnte. Für die Einzelüberwachung waren die Verfassungsschutzämter der Länder, für die allgemeine Überwachung BND und MAD zuständig. Das Bundesamt für Verfassungsschutz übernahm die Post- und Telefonüberwachung im Raum Köln – Bonn, insbesondere die Überwachung der Regierungsstellen, sowie koordinierende Funktionen. Die alliierten Behörden mussten künf-

58 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 217.

59 BArch, B 257/68698, Vermerk des Bundesministers für Post und Fernmeldewesen, 7.5.1968.

tig ihre Überwachungswünsche bei den jeweils zuständigen deutschen Stellen beantragen, für die Einzelüberwachung beim BfV, für die strategische Überwachung beim BND.[60]

Durch das G 10-Gesetz von 1968 war die Situation für die Alliierten keineswegs schlechter, sondern besser geworden. Und das aus drei Gründen:

1. Mit dem G 10-Gesetz konnten zum ersten Mal auch die westdeutschen Geheimdienste in Sachen Post- und Fernmeldeüberwachung umfassend tätig werden. Dadurch stieg das Volumen der deutsch-alliierten Überwachungen erheblich an. In einem Verbund von Bundes- und Landesämtern für Verfassungsschutz, BND und MAD wurde die Bundesrepublik Deutschland mit einem Netz von Überwachungsstellen überzogen, das im Bedarfsfall eine flächendeckende Überwachung des Post- und Fernmeldeverkehrs ermöglichte. Die deutschen Geheimdienste waren durch inzwischen mehrfach abgesicherte Vereinbarungen verpflichtet, alle wichtigen Erkenntnisse, Informationen und Daten den westlichen Geheimdiensten zur Verfügung zu stellen. Nach der gesetzlichen Regelung bekamen die Drei Mächte deutlich mehr Material als je zuvor.

2. Nach dem G 10-Gesetz durften die Alliierten auch weiterhin Überwachungsmaßnahmen durchführen bzw. durchführen lassen. Dies geschah jetzt auf Antrag über die westdeutschen Geheimdienste, die zu Dienstleistern ihrer westlichen Kollegen wurden. Zuständig für die Alliierten in Sachen Postüberwachung war der Verfassungsschutz, in Sachen Fernmeldeüberwachung der BND. Die Anträge wurden an eine, lediglich mit vier Personen besetzte sog. G 10-Kommission des Deutschen Bundestages weitergeleitet und in der Regel anstandslos genehmigt. Danach lösten die westdeutschen Dienste über die Bundespost die Überwachungsmaßnahmen für die Alliierten aus und leiteten das gewonnene Material zur Auswertung an die Amerikaner, Briten oder Franzosen weiter.

3. Die alliierten Geheimdienste konnten auch in Zukunft eigenständig tätig werden und mussten sich keineswegs auf die Dienstleistungen der westdeutschen Geheimdienste beschränken. Dies geschah nicht auf Antrag, sondern aufgrund eigenen Rechts. Als Rechtsgrundlage diente das Selbstverteidigungsrecht der alliierten Truppen auf deutschem Boden.

60 PA AA, B 130/5761, Geheime Verwaltungsvereinbarung zum G10-Gesetz, 22.10.1968.

Wie Konrad Adenauer 1954 musste auch Willy Brandt 1968 in einer eigenen Note das Selbstverteidigungsrecht der alliierten Truppen in der Bundesrepublik als völkerrechtlich sanktioniertes und damit deutsches Recht anerkennen und bestätigen. Danach war jeder Militärbefehlshaber in der Bundesrepublik unabhängig von den sonstigen gesetzlichen Regelungen ermächtigt, „im Falle einer unmittelbaren Bedrohung seiner Streitkräfte die angemessenen Schutzmaßnahmen" zu ergreifen. Diese reichten von der präventiven Überwachung des Post- und Fernmeldeverkehrs über die allgemeine geheimdienstliche Tätigkeit bis zum Gebrauch von „Waffengewalt".[61]

Mit dem G 10-Gesetz, der geheimen Zusatzvereinbarung und der erneut ausgetauschten Note zur Anerkennung des Selbstverteidigungsrechts der Oberkommandierenden der Truppen[62] waren alle bisherigen „Schutzmaßnahmen" und Formen der Überwachung des Post- und Fernmeldeverkehrs auch in Zukunft möglich. Da alle Bundesregierungen diese völkerrechtlichen Vereinbarungen, gesetzlichen Regelungen und geheimen Zusatzvereinbarungen zur Überwachung des Post- und Fernmeldeverkehrs in der Bundesrepublik respektiert und durch neue Vereinbarungen ergänzt haben, ist zusätzlich ein gewohnheitsrechtlicher Anspruch entstanden, der bis in die aktuelle NSA-Affäre hinein nicht ernsthaft in Frage gestellt worden ist. Im Klartext bedeutet dies: Solange es auf deutschem Boden alliierte Truppen, militärische Standorte und Einrichtungen gibt, wird es auf deutschem Boden und von deutschem Boden aus alliierte, insbesondere amerikanische Überwachungsmaßnahmen geben.

Das G 10-Gesetz von 1968 hatte einschneidende verfassungsrechtliche Konsequenzen. Damit die alliierten Geheimdienste und in deren bzw. in eigenem Auftrag auch die deutschen Geheimdienste die individuellen und strategischen Überwachungsmaßnahmen unbehelligt durchführen konnten, bedurfte es strenger Geheimhaltung. Um diese zu garantieren, musste verhindert werden, dass weder der Einzelne, noch die Öffentlichkeit jemals etwas davon erfuhren. Diese Forderung war ohne eine Änderung des Grundgesetzes nicht umzusetzen. Um eine Überwachung des Post- und Fernmeldeverkehrs zu geheimdienstlichen Zwecken zu ermöglichen, mussten fundamentale Grundrechte wie die Unverletzlichkeit des Brief-,

61 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dokument Nr. 18b, S. 298.

62 Ebenda, Dokument Nr. 18b, Punkt 6, S. 298.

Post- und Fernmeldegeheimnisses, die Pflicht, die oder den Überwachten über die Maßnahme des Staates zu informieren, und die Garantie, wonach jedermann, der sich durch die öffentliche Gewalt in seinen Rechten verletzt fühlt, der Rechtsweg offen steht, beschränkt werden.[63]

Entsprechend erhielt Artikel 10 des Grundgesetzes, der die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses garantiert, einen Zusatz, wonach aus Gründen des Staatsschutzes eine entsprechende Beschränkung dieses Grundrechtes möglich ist. „Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.“[64] Mit dieser Grundgesetzänderung wurde faktisch die Gewaltenteilung aufgehoben, die Judikative und das Recht auf gerichtlichen Schutz ausgeschaltet sowie die Legislative ihrer Kontrollfunktion beraubt und auf eine nur wenige Personen umfassende G 10-Kommission reduziert, die nicht einmal den Fraktionsvorsitzenden im Deutschen Bundestag berichten durfte.

Wer gegen das strikte Geheimhaltungsgebot verstieß, lief Gefahr, des Landesverrats angeklagt zu werden. Dies galt auch, seit 1968 verschärfend, für Bundestagsabgeordnete. Parallel zum G 10-Gesetz wurde mit der Verabschiedung des 8. Strafrechtsänderungsgesetzes Paragraph 100 des Strafgesetzbuches in der Fassung von 1951, der – wie wir heute sagen würden – „Whistleblower-Paragraph“, ersatzlos gestrichen. Er lautete: „Ein Abgeordneter des Bundestages, der nach gewissenhafter Prüfung der Sach- und Rechtslage und sorgfältiger Abwägung der widerstreitenden Interessen, sich für verpflichtet hält, einen Verstoß gegen die verfassungsmäßige Ordnung des Bundes oder eines Landes im Bundestag oder in einer seiner Ausschüsse zu rügen, und dadurch ein Staatsgeheimnis öffentlich bekannt macht, handelt nicht rechtswidrig, wenn er mit der Rüge beabsichtigt, einen Bruch des Grundgesetzes oder der Verfassung eines Landes abzuwehren.“[65]

Mit einer denkbar knappen Mehrheit von 5:3 Stimmen billigte das Bundesverfassungsgericht am 15. Dezember 1970 das G 10-Gesetz. Die

63 GG, Art. 19, Abs. 4.

64 GG Art.10 Abs. 2.

65 Bundesgesetzblatt (BGBl.) I (1951), S. 742.

Minderheit der Verfassungsrichter sah dagegen in der Ausschaltung der Informationspflicht und des Rechtsweges für die Betroffenen eine verfassungswidrige Verletzung der Grundrechte und eine Ausschaltung der Gewaltenteilung. „Es ist ein Widerspruch in sich selbst, wenn man zum Schutze der Verfassung unveräußerliche Grundsätze der Verfassung preisgibt.“ [66]

Die deutsch-alliierten Überwachungen seit den 1970er Jahren

Das Bundesverfassungsgericht hatte unter dem Vorsitz seines Vizepräsidenten Walter Seuffert, der bis zu seiner Wahl zum Bundesrichter langjähriges Mitglied der SPD-Bundestagsfraktion gewesen war, eines seiner umstrittensten Urteile gefällt. Erst, nachdem sich der Europäische Gerichtshof 1978 weitgehend der Argumentationslinie der Karlsruher Richter angeschlossen hatte, verstummte die verfassungsrechtliche Diskussion mehr und mehr. Das höchste deutsche Gericht sollte sich noch mehrfach mit dem G 10-Gesetz und seinen zahlreichen Novellierungen beschäftigen. Die Tendenz war stets: ja, aber. Prinzipiell stimmten die Verfassungsrichter den von den verschiedenen Bundesregierungen geforderten Ausweitungen der Rechte und Möglichkeiten der deutschen Geheimdienste zu. So 1984, als das Gericht unter dem Vorsitz von Roman Herzog die strategische, millionenfache Überwachung durch den BND prinzipiell billigte und eine gerichtliche Kontrolle wegen des parlamentarischen Kontrollgremiums nicht für nötig hielt.[67]

Die Siebzigerjahre wurden nicht nur ein Jahrzehnt terroristischer Bedrohungen und nachrichtendienstlicher Affären, sondern auch ein Jahrzehnt der öffentlichen Kritik und Aufklärung der Arbeitsweise der westdeutschen Geheimdienste durch die Medien. Aus zahlreichen Berichten entstand ein Bild von der Wirklichkeit einer überwachten Bundesrepublik, das den Befürchtungen der Kritiker eher entsprach, als der wohlwollenden Sichtweise des Bundesverfassungsgerichts von der stets korrekt und fair handelnden Exekutive. Gab die Praxis der geheimdienstlichen

66 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dokument Nr. 56, S. 361.

67 Entscheidungen des Bundesverfassungsgerichts (BVerfGE), GG Art. 10 I; G 10 §§ 1,3,5,9, S. 125.

Überwachung nicht eher jenen Richtern Recht, die in ihrem Sondervotum von einem Widerspruch in sich sprachen, wenn man zum Schutz der Verfassung unveräußerliche Grundsätze der Verfassung preisgebe?

Deutlich wurde, dass die Überwachung des Post- und Telefonverkehrs keineswegs, wie das G 10-Gesetz es forderte, das letzte aller Mittel war, das erst eingesetzt wurde, nachdem alle übrigen nachrichtendienstlichen Möglichkeiten ausgeschöpft waren. Die individuelle, aber auch die allgemeine Überwachung des Post- und Telefonverkehrs wurde vielmehr sehr schnell und vielfach nach Belieben und ohne Rücksicht auf Recht und Gesetz eingesetzt, wie die öffentlich bekannt gewordenen Fälle, aber auch die durch den Bundesverteidigungsminister angeordneten, allgemeinen Abhörmaßnahmen etwa 1975 im Entführungsfall des Berliner CDU-Politikers Peter Lorenz zeigten. Von einer extremen Gefahrensituation für den inneren oder äußeren Bestand der Bundesrepublik konnte in keinem der Fälle die Rede sein. Das G 10-Gesetz erwies sich somit kaum als ein Ausschließungs- oder Beschränkungsgesetz, sondern als ein Ermöglichungs- und Ermächtigungsgesetz für die westdeutschen und alliierten Geheimdienste, die nachrichtendienstlichen Mittel nach eigenem Gutdünken einzusetzen.

Deutlich wurde, dass G 10-Kommission und G 10-Gremium keineswegs die ordentliche Gerichtsbarkeit ersetzen konnten. Antragsstellung, Entscheidung, Genehmigung und Kontrolle entwickelten sich rasch zu einem ganz normalen bürokratischen Verfahren. Der Chef des jeweiligen Geheimdienstes wählte die Maßnahme aus, das zuständige Ministerium prüfte die formale Korrektheit, und die G 10-Komission stimmte zu. „Da wird weder gefragt noch geprüft, alles geht seinen bürokratischen Gang." Das laufe „so unbürokratisch", wie der SPD-Abgeordnete Jürgen Linde betonte, „dass es einem Angst werden kann"[68].

Deutlich wurde, dass sich die Überwachungsmaßnahmen keineswegs nur auf individuelle Überwachungen beschränkten, sondern dass auch regelmäßig allgemeine Überwachungsmaßnahmen durchgeführt wurden, von denen die Öffentlichkeit erst Anfang der Achtzigerjahre in einem ZEIT-Artikel erfuhr. Diese allgemeinen oder auch strategischen Überwachungen erlaubten es dem BND, jährlich Millionen Postsendungen aus der DDR zu öffnen und auszuwerten.[69] Deutlich wurde erstmals, dass es

68 Der Spiegel, Geheimdienst. Ausgesprochene Dämlacke, 20.11.1978.

69 Der Spiegel, Postgeheimnis. Briefchen im Brief, 23.07.1979.

zweierlei Kontrollen der DDR-Post gab, die des BND und der US-Geheimdienste auf der einen und die der Post- und Zollbeamten nach der Interzonenüberwachungs-Verordnung von 1951 und dem Verbringungsverbotsgesetz von 1961 auf der anderen Seite. Gesetzliche Regelungen, die auch weiterhin in Kraft blieben.[70]

Deutlich wurde, dass Informationen unter den drei Geheimdiensten weitergereicht wurden, auch wenn diese aus einer allgemeinen Überwachung des BND stammten, die laut Entscheidungen des Bundesverfassungsgerichts[71] weder an andere Behörden weitergegeben, noch, wie das Bundesverfassungsgericht 1984 ergänzte, „zur Gefahrenabwehr für die innere Sicherheit" verwendet werden durften.[72] 1970 waren es zum Beispiel „195 Erkenntnisse", die der BND an den MAD in drei Monaten weitergab, während das BfV sogar „140 Informationen" erhielt, die allerdings in den Folgemonaten „auf höchstens 5 bis 6 Erkenntnisse pro Monat" zurückgingen. Der Grund dafür war, wie der BND dem BfV und MAD erklärte, „dass diese Art der Amtshilfe nicht rechtsgemäß war"[73]. Die von den Geheimdiensten, aber auch von der Exekutive wie der G 10-Kommission aufgestellte und vom Bundesverfassungsgericht 1984 übernommene Behauptung, die aus allgemeinen Überwachungsmaßnahmen gewonnenen Informationen eigneten sich nicht für personenbezogene Ermittlungen, entsprach – wie die oben genannten Zahlen zeigen – offensichtlich doch nicht so ganz der Wahrheit.[74]

Deutlich wurde vor allem, dass diejenigen, die Verfassung und Rechtsstaat schützen und verteidigen sollten, aus eben dieser Aufgabe ein höheres Recht für sich ableiteten, das sie bei der Erledigung ihrer Aufgaben zumindest teilweise über geltendes Recht und Gesetz stellten. Während eine kritische Öffentlichkeit hieraus die Notwendigkeit effektiver Kontrollen und Beschränkungen ableitete, verstanden es die Geheimdienste, sich derartigen Kontrollen und gesetzlichen Beschränkungen immer wieder mit dem Hinweis auf äußere und innere Bedrohungen

70 Foschepoth, Überwachtes Deutschland (wie Anm. 1), Quellen-Dokumentation, Dok. Nr. 33 und 34, S. 319-321.

71 BVerfGE 30 (15.12.1970), S. 22.

72 BVerfGE, GG Art. 10 I, 20.06.1984, in: NJW Heft 3, 1985, S. 121.

73 Bundesministerium für Wirtschaft (BMWI), VS-Akten des BMPF, Protokoll über die Sitzung der Arbeitsgruppe der Dienste zu G-10, 09.02.1971.

74 Vgl. Claus Arndt, Die „strategische Kontrolle" von Post- und Fernmeldeverkehrsbeziehungen, in: NJW 1985, S. 107-111, hier S. 107. Arndt war Mitglied der G 10-Kommission.

erfolgreich zu widersetzen. So machten sich die Politiker trotz immer neuer Affären „eher lustlos daran, den deutschen Geheimdienstlern neue Maßstäbe für ihr Treiben zu setzen. Kein verantwortlicher Politiker in Koalition und Opposition mag sich dem Vorwurf der Profis aussetzen, durch klare gesetzliche Regeln die Erfolgschancen der Dienste bei der Gegenspionage gegen Staatsfeinde und Ostagenten zu verringern."[75]

Als Fazit der zahlreichen geheimdienstlichen Affären und der anhaltenden öffentlichen Kritik in den Siebzigerjahren lässt sich festhalten, wie der damalige Bundesgeschäftsführer der FDP, Günter Verheugen, es formulierte: „Die Maßstäbe sind verrutscht, die Grenzen werden fließend."[76]

Dies galt auch für die Entwicklung und die Aktivitäten der amerikanischen Geheimdienste in der Bundesrepublik Deutschland, allen voran der National Security Agency (NSA). Ihr widmete der *Spiegel* 1989 eine große Titelgeschichte. Die NSA habe sich inzwischen zum „aggressivsten US-Nachrichtendienst" entwickelt, so das Magazin. „Von alliierten Sonderrechten ermächtigt und durch Gesetze geschützt, von allzeit schussbereiten Sicherheitskräften bewacht, von kamerabestückten Stacheldrahtzäunen und elektronischen Schutzschilden umhüllt, hat sich die NSA zu einer Monsterorganisation entwickelt, die in einem politischen Vakuum weitgehend nach eigenem Gutdünken operiert."[77]

Nur fünf Prozent aller Geheimdiensterkenntnisse liefere die CIA, so der *Spiegel* weiter. 95 Prozent kämen dagegen von der NSA. In Westberlin arbeiteten nur noch 60 Amerikaner bei der CIA, bei der NSA dagegen 600. Kein Land der westlichen Welt sei für das Aushorchen des östlichen Gegners so gut geeignet wie die Bundesrepublik. „Über 350 geheimdienstliche Zentren, Stäbe und Kommandos der USA" befänden sich auf bundesdeutschem Boden. Eine wichtige Horchstation residiere in Frankfurt, am Fernsprechknotenpunkt der Bundesrepublik. „In der City, zwischen Zeil und Großer Eschersheimer Straße, treffen die meisten Richtfunk- und Leitungsnetze der Post zusammen, die – wie eine liegende Acht – die Republik umspannen."[78]

---

75 Der Spiegel, Geheimdienste. Mit Kanonen, 13.02.1978.

76 Der Spiegel, Georg Lebers Reserven sind verbraucht, 30.01.1978. Das Zitat stammt von dem.

77 Der Spiegel, NSA: Amerikas großes Ohr, 20.02.1989.

78 Ebenda.

Zunächst war die NSA in der obersten Etage des Postscheckamtes Frankfurt untergebracht. Ende der Achtzigerjahre hatte sie sich „Am Hauptbahnhof 6“ eingemietet und firmierte jetzt als „Nebenstelle Frankfurt“ der „Hauptstelle für spezielle Datenverarbeitung“. Wenn diese Angabe stimmt, war die NSA im gleichen Gebäude und unter gleichem Namen in der Frankfurter Stelle für strategische Post- und Fernmeldeüberwachung des BND untergebracht. Es war nämlich der BND, nicht die NSA, wie der *Spiegel* vermutete, der unter dem Tarnnamen „Nebenstelle X der Hauptstelle für spezielle Datenverarbeitung“ in den verschiedenen Städten der Bundesrepublik Deutschland firmierte. Weitere Horchposten unterhielt die NSA in Bad Aibling, nahe Rosenheim, in Gablingen, nördlich von Augsburg, auf dem Arber im Bayerischen Wald, im Elm, einem waldreichen Gebiet zwischen Helmstedt und Wolfenbüttel, und auf dem Teufelsberg in West-Berlin. In diesen Horchstationen der NSA wurde „offenbar mit Wissen und Billigung der Bundesregierung jeder Piepser abgehört“.[79]

Die alliierten Rechte nach der Vereinigung Deutschlands

Die Bedeutung des Jahres 1990 für die Geschichte der Überwachung des Post- und Fernmeldeverkehrs in der Bundesrepublik Deutschland ist schnell erklärt. Alles, was in 40 Jahren Bundesrepublik an deutsch-alliierten Verträgen und Vereinbarungen, deutschen Gesetzen, Regelungen und Erfahrungen zum Aufbau eines im Geheimen operierenden Überwachungsstaates angefallen war, wurde als Erbmasse in die deutsch-deutsche Vereinigung eingebracht. Die Forderung der damaligen oppositionellen SPD an die Regierung Kohl/Genscher dafür zu sorgen, dass mit der Herstellung der Einheit Deutschlands sämtliche Überwachungen des Post- und Fernmeldeverkehrs in der Bundesrepublik und nicht nur die der Sowjetunion, sondern auch die der USA eingestellt würden, wurde ebenso wenig beachtet, wie die Forderung nach Überprüfung und gegebenenfalls Kündigung entsprechender Verträge und Vereinbarungen. Helmut Schäfer, Staatsminister im Auswärtigen Amt, bestätigte stattdessen, dass die Aktivitäten der als militärische Einheiten organisierten US-Geheimdienste auf dem Aufenthaltsvertrag vom 23.10.1954 und den Zusatzvereinbarungen zum NATO-Truppenstatut von 1959 basierten, die in der revidierten Form von 1994 bis heute gültig sind. „Für die Anwendung

79 Der Horchposten auf dem Arber wird im Spiegel nicht erwähnt.

der genannten Verträge auf die in der Bundesrepublik Deutschland stationierten Streitkräfte der Verbündeten", so der Staatsminister weiter, „kommt es allerdings nicht darauf an, ob und in welchem Grad sie in die militärische Befehlsstruktur der NATO eingebettet sind."[80]

Am 12. September 1990 unterzeichneten die Außenminister der vier Siegermächte des Zweiten Weltkriegs und der beiden deutschen Staaten in Moskau den sog. Zwei-Plus-Vier-Vertrag bzw. den „Vertrag über die abschließende Regelung in Bezug auf Deutschland", wie der offizielle Titel lautet. In Artikel 7 erklärten die Vier Mächte ihre Vorbehaltsrechte bezüglich Berlin und Deutschland als Ganzes für beendet. „Das vereinte Deutschland hat demgemäß volle Souveränität über seine inneren und äußeren Angelegenheiten."[81]

Ganz so souverän, wie es diese Formulierung suggerierte, war das neue Deutschland natürlich nicht. Ein Beitritt zu einem von der Sowjetunion dominierten Bündnis wäre von den Westmächten ebenso wenig hinnehmbar gewesen, wie eine Lösung der von der alten Bundesrepublik eingegangenen Westbindungen. Entsprechend wurde im Zwei-Plus-Vier-Vertrag ein Abzug der sowjetischen Truppen aus Deutschland vereinbart und bis zum August 1994 auch vollzogen, ein Abzug der westlichen Truppen aus Deutschland jedoch nicht.

Im Gegenteil. Circa zwei Wochen nach Unterzeichnung des Zwei-Plus-Vier-Vertrags bekräftigten die drei Westmächte und die Bundesrepublik Deutschland durch Notenaustausch vom 25. und 28. September 1990 die Fortgeltung der wichtigsten Verträge und Vereinbarungen zur Westeinbindung der Bundesrepublik aus den Fünfzigerjahren. Die Bundesregierung ließ sich vorab durch Gesetz ermächtigen, entsprechende völkerrechtlich verbindliche Zusagen per Notenaustausch zu machen, was bedeutete, dass die Fortgeltung der Westverträge nicht durch den Bundestag ratifiziert werden musste.

Nach diesen Zusagen blieben teils in gekürzter, teils in geänderter, teils in ergänzter Form für das Vereinte Deutschland in Kraft:

– Aufenthaltsvertrag (1955): Stationierung nach Besatzungsrecht[82],

80 Foschepoth, Überwachtes Deutschland (wie Anm. 1), S. 249.

81 BGBl.1990 II, S. 1317, „Zwei-Plus-Vier-Vertrag", 12.9.1990.

82 BGBl. 1990 II, S. 1390, Notenwechsel zum Aufenthaltsvertrag.

- NEU: Berlin-Vertrag (1990): Aufenthaltsvertrag gilt jetzt auch in Berlin[83],
- Überleitungsvertrag (1955): Alliierte Gesetze bleiben in Kraft[84],
- NATO-Truppenstatut (1951): Beitritt der Bundesrepublik 1955[85],
- Zusatzvertrag NATO-Truppenstatut (1959), revidierte Fassung 1994.[86]

Welche Konsequenzen ergeben sich für unsere Fragestellung aus der vertraglichen Fort- und Festschreibung der Westeinbindung des Vereinten Deutschlands? Der Aufenthaltsvertrag von 1955 stand und steht damit weiterhin unter dem Stationierungsvorbehalt aufgrund der Besetzung Deutschlands, ergänzt um das Recht, das sich aus dem NATO-Beitritt der Bundesrepublik Deutschland ergibt. Die „Effektivstärke" der ausländischen Streitkräfte in der Bundesrepublik, etwa der USA, hängt nicht von der Zustimmung der Bundesregierung ab. Wie viele Streitkräfte stationiert werden dürfen, hängt vom Zeitpunkt „des Inkrafttretens dieser Abmachungen", also am 25. März 1955, ab. Die Effektivstärke der „in der Bundesrepublik stationierten Streitkräfte darf mit Zustimmung der Regierung der Bundesrepublik Deutschland jederzeit erhöht werden".[87] Die Klausel, wonach der Aufenthalts- bzw. Truppenstationierungsvertrag „mit dem Abschluss einer friedensvertraglichen Regelung mit Deutschland" außer Kraft trete[88], wurde durch den Notenwechsel vom 25. September 1990 in ein jederzeitiges Kündigungsrecht der Vertragspartner mit „einer Frist von zwölf Monaten"[89] umgewandelt.

Mit dem Recht auf Stationierung alliierter Truppen in der Bundesrepublik Deutschland sind weiterhin eine Vielzahl von Sonderrechten und Privilegien, besonders der USA als größter, noch in der Bundesrepublik verbliebener ausländischer Streitmacht verbunden. Von bestimmten Zoll- und Steuerprivilegien, über die Beteiligung der Bundesrepublik an den Infrastruktur- und Aufenthaltskosten der amerikanischen Streitkräfte in beträchtlicher Höhe, die Übernahme von Sozialleistungen für deutsche

83 BGBl. 1990 II, S. 1246, Ausweitung Aufenthaltsvertrag auf Berlin.

84 BGBl. 1990 II, S. 1386, Alliiertes Besatzungsrecht gilt als deutsches Recht weiter.

85 BGBl. 1990 II, S.1250. NATO-Truppenstatut bleibt in Kraft.

86 BGBl. 1994 II, S. 2594 Zusatzabkommen zum NATO-Truppenstatut, revidierte Fassung von 1994.

87 BGBl. 1955 II, S. 254, Aufenthaltsvertrag, Art. 1, Abs. 1 und 2.

88 BGBl. 1955 II, S. 254, Aufenthaltsvertrag, Art. 3, Abs. 1.

89 BGBl. 1990 II, S.1252, Notenwechsel vom 25.9.1990, Punkt 11.

Beschäftigte an den US-Standorten[90] bis zur Geltung amerikanischen Rechts auf deutschem Boden. Nicht nur in US-Botschaften und -Konsulaten, sondern auch und vor allem auf allen US-Basen einschließlich des Luftraums darüber gilt amerikanisches Recht, jedenfalls was die Fragen der Sicherheit, des Schutzes der Truppen und der US-Geheimdienste sowie des Straf- und Disziplinarrechts anbetrifft.[91]

Geblieben ist auch die Generalvollmacht zur Überwachung des Post- und Fernmeldeverkehrs von amerikanischen Militärstandorten oder eigens dafür eingerichteten bzw. gemeinsam mit deutschen Geheimdiensten genutzten Abhör- und Überwachungsstationen, jetzt als befriedigende Erfüllung der Verteidigungspflichten beschrieben: „Eine Truppe und ein ziviles Gefolge können innerhalb der ihnen zur ausschließlichen Benutzung überlassenen Liegenschaften die zur befriedigenden Erfüllung ihrer Verteidigungspflichten erforderlichen Maßnahmen treffen."[92] Geblieben ist auch die Verpflichtung beider Seiten zu enger Zusammenarbeit der Geheimdienste zum Sammeln, Austausch und Schutz aller Nachrichten zur Förderung und Wahrung der Sicherheit der Bundesrepublik, der Entsendestaaten und der Truppen sowie deren Staatsangehörigen.[93] Geblieben sind das strikte Geheimhaltungsgebot und die Gleichsetzung und Gleichbehandlung amerikanischer und deutscher Amtsgeheimnisse. Beide Seiten sind danach verpflichtet, alles zu tun, damit Informationen, die die Sicherheit der einen wie der anderen Seiten weder in der Öffentlichkeit, noch vor Gericht jemals bekannt werden.[94]

Die NSA-Affäre, die Echelon Affäre der Neunzigerjahre und viele andere Abhöraffären der USA vorher zeigen, wie umfassend und intensiv die USA von Deutschland aus , aber auch Deutschland selbst überwacht haben und überwachen. Die Duldung der US-amerikanischen Truppen und deren Privilegien einschließlich der intensiven geheimdienstlichen Aktivitäten und Überwachungsmaßnahmen auf deutschem Boden, die enge

90 http://www.sueddeutsche.de/politik/geheimer-krieg-deutschland-zahlt-millionen-fuer-us-militaer-1.1820318 (Oliver Hollenstein, Deutschland zahlt Millionen für US-Militär, abgerufen am 15.11.2014).

91 http://www.sueddeutsche.de/politik/deutsch-amerikanische-beziehungen-in-deutschland-gilt-auch-us-recht-1.2084126 (Josef Foschepoth, In Deutschland gilt auch US-Recht, abgerufen am 15.11.2014).

92 BGBl. 1994 II, S. 2594, Zusatzabkommen zum NATO-Truppenstatut, 1994, Art. 53,1.

93 BGBl. 1961 II, S. 1221, Zusatzabkommen zum NATO-Truppenstatut, Art. 3, Abs. 2.

94 BGBl. 1961 II, S. 1221, Zusatzabkommen zum NATO-Truppenstatut, Art. 38, Abs. 1.

Zusammenarbeit der deutschen und amerikanischen Geheimdienste und die Pflege guter Beziehungen trotz aller Übergriffe der Vereinigten Staaten gehören zur Staatsräson und zur Wirklichkeit der alten und der neuen Bundesrepublik Deutschland.

Völker- und menschenrechtliche Anforderungen an Informationsbeschaffung und Datenüberwachung durch ausländische Geheimdienste

MARKUS KRAJEWSKI

I. Einleitung

Die durch die Enthüllungen von Edward Snowden bekannt gewordenen Abhörmaßnahmen ausländischer Geheimdienste inner- und außerhalb Deutschlands, die mit der sog. Kanzlerin-Handy-Affäre einen Höhepunkt der medialen Aufmerksamkeit erfuhren[1], sind weitgehend aus den öffentlichen Debatten verschwunden. Das dürfte kaum an einem Ende dieser Tätigkeiten, sondern an der zeitlichen Begrenztheit der öffentlichen Aufmerksamkeitsspannen liegen. Die Rechtsprobleme, die mit diesen Tätigkeiten verbunden sind, bestehen jedoch fort und werden in der Fachwissenschaft weiter erörtert. Da es sich bei den US-amerikanischen und britischen Geheimdiensten um Einrichtungen anderer Staaten handelt, die im grenzüberschreitenden Verkehr operieren, liegt es nahe zu fragen, welche völkerrechtlichen Regeln für ausländische Nachrichtendienste insbesondere mit Blick auf den Schutz persönlicher Kommunikation und Daten bestehen. Diese Frage ist in der bisher zu den nachrichtendienstlichen Überwachungen durch ausländische Nachrichtendienste erschienenen Literatur entweder eher kurz behandelt worden oder es wurde die These vertreten, das Völkerrecht trage zur Lösung der Probleme wenig bei.[2]

---

1 Ein knapper Überblick über die wesentlichen Enthüllungen und Ereignisse seit Juni 2013 findet sich bei *Beuth*, Alles Wichtige zum NSA-Skandal, ZeitOnline, 5. Januar 2015, www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/ (Abfrage vom 18.2.2015). Allerdings waren bereits vor 2013 zahlreiche Details des NSA-Programms bekannt, siehe *Sinha*, NSA Surveillance Since 9/11 and the Human Right to Privacy, 59 Loyola Law Review 2014, S. 861 (876 ff.).

2 So etwa *Schmahl*, Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste, Juristenzeitung 2014, S. 220 (221).

Dem soll hier widersprochen werden. Zwar sind die im Folgenden angesprochenen völker- und menschenrechtlichen Verpflichtungen den gleichen Umsetzungsproblemen ausgesetzt wie alle völkerrechtlichen Normen. Die Geltung und Bedeutung des Völkerrechts sollte jedoch nicht mit den gleichen Maßstäben gemessen werden wie das innerstaatliche Verfassungsrecht. Gleichwohl wäre es verkürzt, anzunehmen, völkerrechtliche Schutzmechanismen seien bedeutungslos.

Der Beitrag gliedert sich wie folgt: Ausgehend von der im folgenden Abschnitt (II.) entwickelten Erkenntnis, dass das allgemeine Völkerrecht und die gewohnheitsrechtlichen Grundsätze tatsächlich wenig greifbare Anforderungen an nachrichtendienstliche Tätigkeiten ausländischer Nachrichtendienste enthalten, soll im Anschluss ausführlich der Schutz des Rechts auf Privatheit im globalen Menschenrechtsregime dargelegt werden (III.). Dabei wird gezeigt, dass sich der völkerrechtliche Menschenrechtsschutz in der Vergangenheit als adaptionsfähig gezeigt hat und daher auch geeignet ist, datenschutzrechtliche Standards für das 21. Jahrhundert zu entwickeln. Vor diesem Hintergrund sind auch aktuelle Vorschläge zur legislativen Weiterentwicklung des Völkerrechts deutlich weniger erforderlich als dies gelegentlich angenommen wird. Problematischer erweist sich allerdings die territoriale Verfasstheit des Völkerrechts, die eine Menschenrechtsverletzung, die weder durch personalen Zugriff noch territoriale Verortung gekennzeichnet ist, schwer greifbar macht (IV.). Daran anschließend wird die spezielle Problematik der Abhöraktivitäten, die aus diplomatischen Vertretungen erfolgen, unter dem Gesichtspunkt des Wiener Diplomatenrechts erörtert (V.). Auch hier wird sich zeigen, dass das Völkerrecht über klare Regeln verfügt. Abschließend wird untersucht, welche Rechtsschutzmöglichkeiten betroffenen Staaten und Individuen zur Verfügung stehen (VI.). Dabei erweist sich das in nahezu allen völkerrechtlichen Teilrechtsordnungen anzutreffende Problem der weitgehenden Abwesenheit einer obligatorischen Gerichtsbarkeit als zentrale Herausforderung. Der Beitrag schließt mit einer Zusammenfassung seiner wesentlichen Ergebnisse und einem Ausblick (VII.).

II. Völkerrechtliche Grundlagen der Tätigkeit ausländischer Nachrichtendienste

1. Spionage im Völkerrecht

Völkerrechtliche Überlegungen zu den rechtlichen Anforderungen an die Tätigkeit ausländischer Nachrichtendienste beginnen häufig mit der schlichten Feststellung, dass das Völkerrecht kein umfassendes Spionageverbot kenne.[3] Daran ist richtig, dass der Tatbestand der Nachrichtenbeschaffung durch ausländische Geheimdienste im geltenden Völkerrecht jedenfalls zu Friedenszeiten[4] keiner generellen Einschränkung unterworfen ist.[5] Man kann dies entweder unter Rückgriff auf das sog. Lotus-Prinzip, wonach im Völkerrecht aufgrund der unbeschränkten staatlichen Souveränität alles erlaubt ist, was nicht ausdrücklich verboten ist, begründen oder einen völkergewohnheitsrechtlichen Erlaubnistatbestand aus der allgemein verbreiteten Praxis der Spionage („I spy, you spy, everybody spies“[6]) konstruieren.[7] Das Ergebnis bleibt das gleiche und ist ebenso unbestritten wie trivial.

Wer sich mit der Feststellung, dass Spionage völkerrechtlich nicht verboten ist, begnügt, übersieht jedoch, dass zwischen dem „ob“ und dem „wie“ – wie oft im Recht – zu unterscheiden ist.[8] Spionage findet nicht im

---

3 *Ewer/Thienel,* Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, Neue Juristische Wochenschrift 2014, S. 30 (31); *Talmon*, Das Abhören der Kanzlerhandys und das Völkerrecht, Bonner Rechtsjournal 2014, S. 6 (6); *Schmahl* (Fn. 2), S. 222.

4 In einem bewaffneten Konflikt gelten dagegen die Regeln des humanitären Völkerrechts über Spionage, die in Art. 29 ff. der Haager Landkriegsordnung und Art. 46 des Zusatzprotokolls I (1977) zu den Rotkreuzabkommen niedergelegt sind. Dazu *Sule*, Spionage, 2006, S. 63 ff.

5 Das ist jedenfalls Stand der herrschenden Lehre und Praxis; siehe *Sule* (Fn. 4), S. 73.

6 Vgl. *Wiedrich*, I spy, you spy … everybody spies, Chicago Tribune, 11. April 1975, S. 4. Ebenso *Talmon* (Fn. 3), S. 12.

7 *Schaller*, Spies, Max Planck Encyclopedia of Public International Law, http://opil.ouplaw.com/home/EPIL, 2009, Abs. 2. Gegen ein gewohnheitsrechtliches Recht *Peters*, Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I, EJIL: Talk!, http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/ (Abfrage vom 18.2.2015). Zum Ganzen *Sule* (Fn. 4), S. 74 ff.

8 In diesem Sinne auch *Sule* (Fn. 4), S. 77.

rechtsfreien Raum statt. Der Staat, auf dessen Territorium Spionage stattfindet, ist nicht gehindert, sein eigenes Recht gegenüber dem Spion durchzusetzen und in diesem Rahmen Spionage auch unter Strafe zu stellen (so etwa im deutschen Recht in §§ 93 ff. StGB).[9] Zudem setzt auch die territoriale Souveränität der Spionage Grenzen: Erfolgt die nachrichtendienstliche Ermittlung mit hoheitlichen Maßnahmen (z. B. durch das Abhören von Telefonaten[10] oder durch gewaltsame Befragungen), verletzt sie die Gebietshoheit des Staates, auf dessen Territorium sie stattfinden und stellt damit auch ein Verstoß gegen dessen Souveränität und eine Verletzung des Grundsatzes der Nichteinmischung in innere Angelegenheiten dar.[11] Beschränkt sich die nachrichtendienstliche Tätigkeit dagegen auf das freiwillige Befragen von Auskunftspersonen, liegt kein Verstoß vor. Hoheitliche Maßnahmen sind dagegen grundsätzlich nur mit Zustimmung des Territorialstaats zulässig.

Völkerrechtlich noch ungeklärt ist, ob als Anknüpfungspunkt für Ermittlungstätigkeiten mit hoheitlichen Mitteln auch potentielle Auswirkungen auf das Inland, z. B. bei einer drohenden Gefahr terroristischer Anschläge, genügen. Im Völkerrecht ist die Auswirkung einer Handlung bislang nur in wenigen Konstellationen als zulässiger Anknüpfungspunkt von Hoheitsgewalt anerkannt (Wirkungsprinzip). Über Spionagetätigkeiten ist in diesem Kontext bislang noch nicht ausführlich diskutiert worden.[12] Selbst wenn man dies grundsätzlich zulässt, muss gefragt werden, welchen Grenzen die Berufung auf das Auswirkungsprinzip unterliegt. Zur Beantwortung lässt sich eine Parallele zur Diskussion um die präventive (antizipatorische) und die präemptive Selbstverteidigung ziehen.[13] Während die Maßnahmen, die der allgemeinen Prävention dienen und

9 *Hettel/Kirschhöfer*, Aus aktuellem Anlass: Die Strafbarkeit geheimdienstlicher Spionage in der Bundesrepublik Deutschland, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2014, S. 341 (342 ff.).

10 Zum Sonderfall der nachrichtendienstlichen Tätigkeit aus diplomatischen Missionen siehe unten V.

11 So auch *Ewer/Thiel* (Fn. 3), S. 31; *Schaller* (Fn. 7), Abs. 2. A.A. wohl *Schmahl* (Fn. 2), S. 222. Nach der Beeinträchtigung des staatlichen Gewaltmonopols differenzierend *Sule* (Fn. 6), S. 83 ff.

12 In diese Richtung aber *Peters* (Fn. 7). Siehe auch *Peters*, „Es gibt kein explizites Verbot der Spionage. Aber das heißt nicht, dass sie erlaubt ist.", VerfBlog, 2013/10/31, http://www.verfassungsblog.de/es-gibt-kein-explizites-verbot-spionage-aber-heisst-nicht-dass-erlaubt-ist (Abfrage vom 18.2.2015).

13 *Von Arnauld*, Völkerrecht, 2. Aufl., 2014, Rn. 1065 ff.

sich nicht auf einen unmittelbar bevorstehenden Angriff beziehen, sich nach herrschender Meinung nicht als Selbstverteidigung rechtfertigen lassen, können Handlungen, die einen unmittelbar bevorstehenden Angriff abwehren, gerechtfertigt werden. Entsprechend können Verletzungen der Gebietshoheit durch Spionagetätigkeiten gegebenenfalls als Notstandshandlung gem. Art. 25 des Entwurfs der Völkerrechtskommission für die Staatenverantwortlichkeit gerechtfertigt werden, wenn dadurch unmittelbar bevorstehende Gefahren gegen den spionierenden Staat abgewehrt werden könnten.

Einen Sonderfall stellt möglicherweise das Abhören von Gesprächen von Regierungsmitgliedern dar. Dieses könnte unabhängig von seiner sonstigen Qualifikation in jedem Fall gegen das Interventionsverbot verstoßen, da es die Vertraulichkeit des Gesprächs zwischen Regierungsmitgliedern beeinträchtigt und damit in die inneren Angelegenheiten des Staats eingreift.[14] Allerdings wird man hier differenzieren müssen: Die bloße Informationsbeschaffung, die nicht auf die Beeinflussung staatlichen Handelns abzielt, dürfte nur eine geringe Interventionswirkung entfalten. Da das Abhören von Regierungsmitgliedern jedoch nur selten der „reinen Informationsbeschaffung" dienen dürfte, erscheint es nicht fernliegend, hierin grundsätzlich einen Verstoß gegen das Interventionsverbot zu sehen.

2. No-Spy-Abkommen als rechtliche Einhegung von Nachrichtendiensten?

In den politischen Auseinandersetzungen über die NSA-Affäre war immer wieder die Forderung nach einem völkerrechtlichen Abkommen zwischen den USA und Deutschland, das wechselseitiges Spionieren ausschließen soll, laut geworden. Zeitweise wurde der Eindruck verbreitet, ein derartiges Abkommen stehe unmittelbar bevor.[15] Allerdings bestand seitens der USA hieran kein Interesse, so dass ein No-Spy-Abkommen auf absehbare Zeit nicht auf der Tagesordnung steht.[16]

14 *Ewer/Thienel* (Fn. 3), S. 31; *Peters* (Fn. 7).

15 *Talmon* (Fn. 3), S. 7.

16 *Ganslmeier*, Cyber-Dialog statt No-Spy-Abkommen, tagesschau.de, 19.5.2014, http://www.tagesschau.de/ausland/cyberdialog100.html (Abfrage vom 18.2.2015).

Zwar wäre es grundsätzlich möglich, dass sich zwei oder mehrere Staaten dazu verpflichten, wechselseitig keine Spionageaktivitäten durchzuführen. Allerdings gibt es hierzu bislang noch praktisch keine internationale Praxis. Genannt wird zumeist ein Abkommen zwischen den USA und Großbritannien aus dem Jahre 1946, das durch spätere Beitritte von Australien, Neuseeland und Kanada (sog. „Five Eyes") erweitert wurde. Tatsächlich enthält das Abkommen jedoch kein ausdrückliches Verbot der wechselseitigen Spionage, sondern in erster Linie Verpflichtungen zur Kooperation und zum Informationsaustausch zwischen den Nachrichtendiensten der beteiligten Staaten.[17] Ob dies gegenseitiges Spionieren überflüssig macht[18], ist fraglich, in der Sache jedenfalls kaum überprüfbar. Unabhängig davon dürfte die Effektivität eines sog. No spy-Abkommens dadurch erheblich erschwert werden, dass ein Rechtsverstoß kraft Natur der Sache im Verborgenen geschieht und nur durch eigene Gegenspionage – und damit ebenfalls rechtswidrig – aufgedeckt werden könnte.

III. Menschenrechtlicher Schutz persönlicher Daten und Kommunikation

Anders als das allgemeine Völkerrecht und mögliche völkerrechtliche Einschränkungen der Spionagetätigkeit an sich besteht inzwischen ein ausgeprägtes System internationaler Menschenrechte, das als Schranke für nachrichtendienstliche Tätigkeiten ausländischer Geheimdienste ergiebiger ist.

1. Rechtliche Grundlagen

Sedes materiae des völkerrechtlichen Daten- und Kommunikationsschutzes ist Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR), des sog. Zivilpakts, vom 16. Dezember 1966.[19] Dieser 1976 in Kraft getretene völkerrechtliche Vertrag ist für seine 168 Vertragspar-

17 Siehe die Dokumentation der NSA, UKUSA Agreement Release 1940-1956, unter https://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf (Abfrage vom 18.2.2015).

18 So *Talmon* (Fn. 3), S. 7.

19 *Hoffmann-Riem*, Freiheitsschutz in globalen Kommunikationsinfrastrukturen, Juristenzeitung 2014, S. 53 (62); *Ewer/Thienel* (Fn. 3), S. 32.

teien, unter ihnen alle EU-Mitgliedstaaten und die USA[20], rechtlich bindend. Nach seinem Absatz 1 darf niemand willkürlichen Eingriffen in sein Privatleben („privacy") und in seinen Schriftverkehr („correspondence") ausgesetzt werden. Nach Absatz 2 hat jedermann Anspruch auf rechtlichen Schutz gegen solche Eingriffe.

Artikel 17 IPbpR beruht auf dem nahezu wortgleichen Art. 12 der Allgemeinen Erklärung der Menschenrechte von 1948 und findet Entsprechungen in Artikel 8 der Europäischen Menschenrechtskonvention von 1950[21] sowie Artikel 11 der Amerikanischen Menschenrechtskonvention von 1969.[22] Der Schutz der Privatheit und des Schriftverkehrs wird auch in Artikel 21 der Arabischen Charta der Menschenrechte von 2004 verankert. Lediglich die Afrikanische Charta der Menschenrechte und Rechte der Völker von 1981 kennt keinen ausdrücklichen Schutz der Privatheit. Da mit Ausnahme des Südsudan jedoch alle Staaten Afrikas den IPbpR ratifiziert haben, besteht hier materiell-rechtlich keine wirkliche Schutzlücke. Problematischer wirkt sich die Abwesenheit eines verbindlichen regionalen Menschenrechtsabkommens in Asien aus, da mehrere asiatische Staaten den IPbpR nicht ratifiziert haben.[23] Im Folgenden steht Art. 17 IPbpR im Mittelpunkt der Überlegungen, da an ihn auch die USA gebunden sind. Im Verhältnis zum Vereinigten Königreich und zu anderen europäischen Staaten ist darüber hinaus Art. 8 Europäische Menschenrechtskonvention (EMRK) und die dazu ergangene Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) einschlägig.

Der für die Auslegung und Umsetzung des Internationalen Pakts über bürgerliche und politische Rechte zuständige Menschenrechtsausschuss hat sich bereits 1988 in seiner Allgemeinen Anmerkung Nr. 16 mit Artikel 17 IPbpR befasst und darin unter anderem festgehalten: „Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited" und „The gathering and holding of per-

---

20 Stand 31. Januar 2015; siehe https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (Abfrage vom 17.2.2015).

21 *Hanschmann*, Das Verschwinden des Grundrechts auf Datenschutz gegen hoheitliche Maßnahmen in der Pluralität von Rechtsregimen, in: Matz-Lück/Hong (Hrsg.), Grundrechte und Grundfreiheiten im Mehrebenensystem, 2012, S. 293 (300 ff.).

22 *Ziemele*, Privacy, Right to, International Protection, Max Planck Encyclopedia of Public International Law, http://opil.ouplaw.com/home/EPIL, 2009, Abs. 9 ff.

23 Dazu zählen China, Malaysia und Myanmar.

sonal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."[24]

Damit hat der Menschenrechtsausschuss zum einen deutlich gemacht, dass der Begriff „correspondence" weit auszulegen ist und nicht nur den klassischen Brief- oder Fernmeldeverkehr erfasst, sondern auch moderne elektronische Kommunikationsformen. Zum anderen betont der Ausschuss, dass der Schutz von personenbezogenen Daten durch das Recht auf Privatheit geschützt wird. Der menschenrechtliche Daten- und Kommunikationsschutz ist daher Teil des Rechts auf Privatheit und der Freiheit der Korrespondenz.[25] In ihrem Bericht an die Generalversammlung „The right to privacy in the digital age" aus dem Jahre 2014 hat die damalige UN-Hochkommissarin für Menschenrechte, Navi Pillay, jede Form des Eingriffs in den Kommunikationsvorgang, auch wenn es sich um das Sammeln von aggregierten Daten („Big data") handelt, als Eingriff in das Recht auf Privatheit bezeichnet.[26] Staatliche Überwachungsmaßnahmen seien nur dann völkerrechtlich legitim, wenn sie die menschenrechtlichen Anforderungen des Art. 17 IPbpR beachten.[27] In diesem Bericht wurde auch betont, dass der Datenschutz nicht nur durch zielgerichtete staatliche Ausforschungen gefährdet ist, sondern zunehmend auch durch die „freiwillige" Preisgabe von Daten im Internet.[28]

Ein enger Zusammenhang besteht auch zum Menschenrecht auf Meinungsfreiheit, das etwa in Art. 19 IPbPR verankert ist.[29] So hat der Sonderberichterstatter der Vereinten Nationen für die Meinungsfreiheit,

---

24 Human Rights Committee, General Comment No. 16 - Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), Twenty-third session, 1988, Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), Abs. 8 und 10.

25 So auch *Nowak*, UN Covenant on Civil and Political Rights. CCPR Commentary, 2005, S. 401, und *Schiedermair,* Der Schutz des Privaten als internationales Grundrecht, 2012, S. 81 f.

26 Human Rights Council, The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30. Juni 2014, Abs. 18 und 19.

27 The right to privacy in the digital age (Fn. 26), Abs. 15.

28 The right to privacy in the digital age (Fn. 26), Abs. 18.

29 *Hoffmann-Riem* (Fn. 19), S. 62.

Frank LaRue, bereits 2011 deutlich gemacht, dass der mangelnde Datenschutz im Internet sowie die staatliche Überwachung des Internets und der Informationsbeschaffung über Internet-Kommunikationen auch die Ausübung der Meinungsfreiheit beeinträchtigen kann.[30]

2. Rechtfertigungen von Eingriffen in das Recht auf Privatheit und Datenschutz

Aus dem oben Gesagten lässt sich zunächst ableiten, dass das Abhören, Speichern und Verwerten von höchstpersönlichen Daten und Kommunikation durch Polizei, Sicherheitskräfte und Nachrichtendienste einen Eingriff in das Recht auf Privatheit und den Schutz der Korrespondenz darstellt. So besteht auch weitgehend Einigkeit, dass die USA und alle Vertragsparteien des Zivilpakts das Recht auf Privatheit beachten müssen, wenn ihre Nachrichtendienste auf persönliche Daten und Informationen von natürlichen und juristischen Personen zugreifen.[31]

Das Recht auf Privatheit und der Schutz der privaten Kommunikation nach Art. 17 IPbpR und den regionalen Menschenrechtskonventionen gelten allerdings nicht absolut.[32] Interessanterweise sieht Art. 17 IPbpR – anders als Art. 8 EMRK – keinen allgemeinen Schrankenvorbehalt vor, der Eingriffe rechtfertigen könnte. Allerdings ist anerkannt, dass sich aus der Formulierung, dass „keine willkürlichen oder rechtswidrigen Eingriffe" gestattet sind, ein Rechtfertigungstatbestand ableiten lässt, mit dem willkürliche und rechtswidrige von rechtmäßigen Eingriffen unterschieden werden können.[33]

In der Praxis des Menschenrechtsausschusses wurden diese Anforderungen ähnlich ausgelegt wie die im Zivilpakt explizit angelegten Recht-

30 Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16. Mai 2011, Abs. 53 ff.

31 *Peters*, Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II, EJIL: Talk!, http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ (Abfrage vom 18.2.2015); *Fischer-Lescano*, Der Kampf um die Internetverfassung, Juristenzeitung 2014, S. 965 (969); *Ewer/Thienel* (Fn. 3), S. 32; *Schmahl* (Fn. 2), S. 222.

32 General Comment No. 16 (Fn. 24), Abs. 7: „As all persons live in society, the protection of privacy is necessarily relative."

33 The right to privacy in the digital age (Fn. 26), Abs. 22; *Nowak* (Fn. 25), S. 381; *Fischer-Lescano* (Fn. 31), S. 970.

fertigungsklauseln. Demnach sind Eingriffe in die Privatheit und den Schutz privater Kommunikation gerechtfertigt, wenn sie auf einer gesetzlichen Grundlage erfolgen und die gesetzlichen Ziele mit Zweck und Ziel des Zivilpakts vereinbar sind.[34] Hierzu zählt grundsätzlich auch das von den meisten Staaten angebrachte Ziel der inneren und äußeren Sicherheit.[35] Entsprechend wird in Teilen des US-amerikanischen Schrifttums auch die Auffassung vertreten, die Überwachungsmaßnahmen der NSA seien gerechtfertigt.[36]

Allerdings sind Maßnahmen, die in das Recht auf Privatheit und den Schutz der privaten Korrespondenz eingreifen, einem strikten Verhältnismäßigkeitstest unterworfen.[37] Dabei sind vor allem die Erforderlichkeit und die Angemessenheit im Einzelnen kritisch zu prüfen. Bei anlasslosen massenhaften Überwachungen von Daten dürfte jedenfalls die Erforderlichkeit zweifelhaft sein.[38] Schließlich ist daran zu erinnern, dass Eingriffe in die Rechte gem. Art. 17 Abs. 1 IPbpR einer gerichtlichen Überprüfung und Kontrolle zugängig gemacht werden müssen (Art. 17 Abs. 2 IPbpR). Eine innerbehördliche Überprüfung ohne gerichtliche oder gerichtsähnliche Verfahren dürfte nicht ausreichend sein.[39]

3. Datenüberwachung aus dem Ausland und die extraterritoriale Wirkung des Rechts auf Privatheit

Während bezüglich des Inhalts des Menschenrechts auf Privatheit und Vertraulichkeit der Kommunikation noch weitgehend Einigkeit besteht und sich der Streit im Wesentlichen darauf bezieht, unter welchen Bedingungen dieses Recht aus Gründen der inneren und äußeren Sicherheit

34 Dass dies bei den Abhörprogrammen der USA der Fall ist, bezweifeln *Ewer/Thienel* (Fn. 3), S. 32.

35 The right to privacy in the digital age (Fn. 26), Abs. 24.

36 *Margulies*, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, 82 Fordham International Law Review 2014, S. 2137 (2152 ff.). Differenzierend *Paust*, Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect, 15 Chicago Journal of International Law 2015, S. 612 (638 ff.). Eine Übereinstimmung mit Art. 17 IPbpR bezweifelt *Sinha*, (Fn. 1), S. 943.

37 *Milanovic*, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, 55 Harvard International Law Journal 2014 (im Erscheinen).

38 The right to privacy in the digital age (Fn. 26), Abs. 25.

39 Ähnlich *Ewer/Thienel* (Fn. 3), S. 32.

eingeschränkt werden darf, ist die territoriale Reichweite dieses Rechts in Praxis und Literatur ungeklärt und umstritten.

Ausgangspunkt der Überlegungen ist, dass der Zugriff ausländischer Geheimdienste auf personenbezogene Daten und Kommunikationen nicht zwingend eine physische Präsenz von Mitarbeitern und Technologie auf dem Gebiet des Staates erfordert, in dem sich die Personen aufhalten, deren Kommunikation überwacht wird. Während die klassische Telefonüberwachung einen Zugriff auf die entsprechende Telekommunikationsinfrastruktur erforderte und insofern territorial operieren musste, ist dies bei elektronischer Kommunikation durch Internet nicht mehr erforderlich, da die der Kommunikation zugrunde liegenden elektronischen Signale weltweit verschickt werden und daher auch extraterritorial abgefangen werden können. So zeichnen sich die Überwachungssysteme der USA „PRISM" und Großbritanniens „Tempora" u. a. dadurch aus, dass sie auf Datenkabel und -infrastruktur, die sich auf ihrem Territorium befinden, zugreifen können und auf diese Weise auf Kommunikationen zugreifen können, deren Teilnehmer sich gar nicht auf ihrem Territorium befinden. Das ist zunächst dann der Fall, wenn die Diensteanbieter (z. B. Internetprovider) ihren Sitz in den USA oder Großbritannien haben. Aber auch sonst, läuft ein Großteil der globalen elektronischen Kommunikation über die USA. Dies hat mit den technischen Entwicklungen von Kommunikation im Internet-Zeitalter zu tun: Eine e-mail, die von Paris nach Berlin gesendet wird, nimmt nicht zwingend den physisch direkten und kürzesten Weg, sondern regelmäßig den kostengünstigsten und dieser führt oft über Kommunikationsinfrastruktur in den USA.[40]

In rechtlicher Hinsicht wirft dies die Frage der extraterritorialen Wirkung von Menschenrechten auf. Menschenrechte gelten grundsätzlich für Personen, die sich im Hoheitsgebiet des Staates befinden oder „seiner Herrschaftsgewalt" unterstehen, so z. B. Art. 2 Abs. 1 IPbpR. Die Personen, in deren Kommunikation oder Daten eingegriffen wird, befinden sich jedoch regelmäßig nicht auf dem Hoheitsgebiet der USA und unterstehen auch nicht deren Hoheitsgewalt im klassischen Sinne.[41] Damit offenbart sich die – auch für das nationale Verfassungsrecht bereits problematisierte[42] – Frage nach der territorialen Bezogenheit einer Rechtsverletzung. Im

40 *Margulies* (Fn. 36), S. 2151.

41 *Paust* (Fn. 36), S. 622 ff.

42 *Hoffman-Riem* (Fn. 19), S. 55 f.

Völkerrecht ist zwar grundsätzlich anerkannt, dass Hoheitsgewalt im Sinne des Art. 2 Abs. 1 IPbpR auch extraterritorial ausgeübt werden kann.[43] Dazu muss der Staat jedoch entweder über ein fremdes Territorium Herrschaftsgewalt ausüben – wie im Fall einer militärischen Besatzung – oder die betroffene Person befindet sich in der physischen Gewalt des Staates wie im Fall von extraterritorialen Gefängnissen.[44]

Es stellt sich daher die Frage, ob die Telefonüberwachung durch Fernaufklärung oder das Abfangen von Internetkommunikation hiervon erfasst sind. Nach dem traditionellen Verständnis von Hoheitsgewalt ist dies zu verneinen, da Menschenrechtsverletzungen die direkte Zugriffsmöglichkeit eines Staats auf eine Person voraussetzen.[45] Lässt man dagegen eine „virtuelle Kontrolle" ausreichen, kann man von Hoheitsgewalt sprechen, wenn auf die Kommunikationsdaten einer Person zugegriffen werden kann.[46] Hierfür spricht, dass die Gefährdungslage bei der elektronischen Überwachung und dem Eingriff in die Vertraulichkeit der Kommunikation nicht dadurch größer wird, dass sich die kontrollierende Stelle und die überwachte Person in physischer Nähe zueinander aufhalten. Auch erfordert die elektronische Überwachung gerade nicht, dass die zu überwachende Person der Jurisdiktionsgewalt des überwachenden Staats ausgesetzt ist.[47] Vielmehr verwirklicht sich die Menschenrechtsverletzung bereits in der – oft anlasslosen – Realisierung der technischen Eingriffsmöglichkeit.[48]

In ihrem Bericht „The right to privacy in the digital age" wies die Hochkommissarin noch auf ein weiteres Argument hin: Ein Staat könne

---

43 Internationaler Gerichtshof, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ Reports 2004, S. 136 (179 ff.). Die USA vertreten allerdings die Auffassung, dass der Zivilpakt überhaupt keine extraterritoriale Wirkung entfaltet; siehe *Sinha* (Fn. 1), S. 901, *Milanovic* (Fn. 37) und *Margulies* (Fn. 36), S. 2143.

44 Ausführlich dazu auch *Talmon*, Der Begriff der „Hoheitsgewalt" in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste, Juristenzeitung 2014, S. 783 (784).

45 *Paust* (Fn. 36), S. 625, und *Talmon* (Fn. 44), S. 784-785, der auch darauf abstellt, dass andernfalls eine unübersehbar große Zahl an Personen Individualbeschwerde erheben könnte.

46 *Margulies* (Fn. 36), S. 2150. In diesem Sinne auch *Milanovic* (Fn. 37), *Peters* (Fn. 31) und *Fischer-Lescano* (Fn. 31), S. 969.

47 *Margulies* (Fn. 36), S. 2151.

48 Vgl. The Guardian, Editorial, NSA and GCHQ: snooping because we can, 20.12.2013: „We are spying not because we need to or should but because we can".

sich seiner menschenrechtlichen Pflichten nicht dadurch entziehen, dass er eine in seinem Territorium unzulässige Maßnahme extraterritorial durchführe. Daraus folge, dass die Staaten bei digitalen Überwachungen ohne territoriale Einschränkung an die Menschenrechte gebunden seien, solange sie die technischen Überwachungsmöglichkeiten effektiv kontrollierten: „Digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure."[49] Von dieser Grundhaltung scheint auch der Menschenrechtsausschuss ausgegangen zu sein, als er im März 2014 seine abschließenden Anmerkungen zum Staatenbericht der USA veröffentlichte.

4. Überprüfung durch den Menschenrechtsausschuss

Der Menschenrechtsausschuss ist gem. Art. 28 ff. IPbpR für die Überwachung und Einhaltung des Zivilpakts zuständig. Dazu stehen ihm verschiedene Verfahren zur Verfügung. Zu den wichtigsten zählen die Einholung und Bewertung von Staatenberichten, die die Vertragsparteien dem Ausschuss vorlegen müssen.[50] Die Berichte werden in regelmäßigen Abständen vorgelegt, auf die dann konkrete Fragen des Ausschusses folgen. Das jüngste entsprechende Verfahren mit den USA wurde 2014 abgeschlossen. Die Überwachungstätigkeiten der NSA wurden dabei auch thematisiert.

Bereits in ihrem 2012 eingereichten Staatenbericht hatten die USA mit Blick auf Art. 17 IPbpR auf die nachrichtendienstliche Auslandsüberwachung hingewiesen, dies jedoch nicht als grundsätzliches Problem aus menschenrechtlicher Sicht angesehen.[51] Der Ausschuss gab sich mit den Ausführungen nicht zufrieden und bat um spezielle Informationen zur gerichtlichen Überwachung der Tätigkeiten der NSA.[52] In ihrer Antwort

49 The right to privacy in the digital age (Fn. 26), Abs. 34.

50 *Schilling*, Internationaler Menschenrechtsschutz, Tübingen 2004, S. 243 ff; *von der Wense*, Der UN-Menschenrechtsausschuß und sein Beitrag zum universellen Schutz der Menschenrechte, Heidelberg 1999, S. 36 ff.

51 Human Rights Committee, Fourth periodic report: United States of America, CCPR/C/USA/4, 22. Mai 2012, Abs. 330 ff.

52 Human Rights Committee, List of issues in relation to the fourth periodic report of the United States of America, CCPR/C/USA/Q/4, 29. April 2013, Abs. 22.

verwiesen die USA auf den Foreign Intelligence Surveillance Court (FISC) und begrüßten eine Diskussion mit dem Ausschuss über die Abwägung von Menschenrechten und nationaler Sicherheit.[53] Zu diesem Zeitpunkt waren die Enthüllungen von Edward Snowden allerdings schon bekannt. Es kann daher davon ausgegangen werden, dass diese auch in den mündlichen Diskussionen des Ausschusses mit den USA eine Rolle gespielt haben.

In seinen Abschließenden Bemerkungen („Concluding observations") zum Staatenbericht der USA vom 26. März 2014 setzt sich der Ausschuss jedenfalls ausführlich mit der Datenüberwachung auseinander.[54] Der Ausschuss zeigte sich besorgt über die Praxis der Überwachung innerhalb und außerhalb der USA und die sich hieraus ergebende Beeinträchtigung des Rechts auf Privatheit. Auch die Tatsache, dass der FISC im Geheimen getagt hatte, wurde kritisiert. Der Ausschuss vertrat die Auffassung, dass das gegenwärtige Überprüfungssystem für die Maßnahmen der NSA die Menschenrechte der betroffenen Personen nicht hinreichend schütze und dass den Betroffenen der Zugang zu effektivem Rechtsschutz fehle. Der Ausschuss forderte die USA daher auf, alle notwendigen Maßnahmen durchzuführen, um die Überwachungsmaßnahmen in Einklang mit dem Zivilpakt zu bringen und zwar unabhängig von der Staatsangehörigkeit und dem Aufenthaltsort von Personen, deren Kommunikation direkt überwacht werde. Zudem müssten die einzelnen Anforderungen an das Recht auf Privatheit gewährt und das gegenwärtige System der Überwachung reformiert werden.

Auch wenn diese Bemerkungen des Ausschusses nicht verbindlich sind, sollten ihre Wirkungen nicht unterschätzt werden. Die USA müssen zwar erst in einigen Jahren wieder dem Ausschuss berichten. Bis dahin werden die Ausführungen des Ausschusses jedoch den politischen Diskurs in den USA beeinflussen und können von kritischen gesellschaftlichen Gruppen unterstützt werden.[55] Ebenso wichtig ist, dass der Ausschuss mit seinen Bemerkungen zur Auslegung des Zivilpakts beiträgt. Diesbezüglich sind zwei Aspekte bedeutsam: Zum einen hat der Ausschuss klar herausgestellt, dass der effektive Rechtsschutz gegen Überwa-

53 Human Rights Committee, Replies of the United States of America to the list of issues, CCPR/C/USA/Q/4/Add.1, 13. September 2013, Abs. 115 ff.

54 Human Rights Committee, Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23. April 2014, Abs. 22.

55 Ähnlich *Fischer-Lesacno* (Fn. 31), S. 968.

chungsmaßnahmen durch öffentliche und unabhängige Gerichte für das Recht auf Privatheit von essentieller Bedeutung ist. Zum anderen wurde durch den Hinweis, dass dieses Menschenrecht unabhängig von Staatsangehörigkeit und Aufenthalt der Betroffenen zu schützen sei, verdeutlicht, dass der Ausschuss eine extraterritoriale Geltung dieses Rechts jedenfalls bei elektronischen Überwachungen für gegeben hält. Damit dürfte der Ausschuss zumindest bei Verletzungen von Art. 17 IPbpR durch im Ausland tätige Nachrichtendienste von einem weiten Verständnis von Hoheitsgewalt im Sinne des Art. 2 (1) IPbpR ausgehen.

IV. Neue rechtspolitische Initiativen

Auf dem Höhepunkt der medialen Aufmerksamkeit und der politischen Diskussionen über die Reaktionen auf die NSA-Enthüllungen wurden auch Forderungen laut, den Zivilpakt durch ein Zusatzprotokoll zum Recht auf Privatsphäre im Internetzeitalter zu ergänzen.[56] Die Bundesregierung griff einen derartigen Vorschlag des damaligen Bundesdatenschutzbeauftragten Peter Schaar im Sommer 2013 auf und regte ein solches Zusatzprotokoll mit dem Argument an, der Menschenrechtsschutz müsse auch den Datenschutz im Internet erfassen.[57] Allerdings stieß dieser Vorschlag international auf wenig Zustimmung und wurde daher nicht weiter verfolgt.

Tatsächlich wäre ein weiteres Zusatzprotokoll zum Zivilpakt in der Sache auch kontraproduktiv gewesen. Zunächst hätte es nur Geltung für die Staaten entfaltet, die ihm ausdrücklich zugestimmt hätten. Es ist nicht anzunehmen, dass die Staaten, deren Geheimdienste umfassend elektronische Daten und Kommunikation überwachen, dem Protokoll beigetreten wären.[58] Diese Staaten hätten dann sogar darauf verweisen können, dass ihre Geheimdienste nicht gegen für sie geltende Menschenrechte verstoßen würden. Weiterhin wäre auch das Verhältnis eines neuen Protokolls zu Art. 17 IPbpR unklar gewesen. Insbesondere da dieser nach dem Verständnis des Menschenrechtsausschusses den Datenschutz im Inter-

56 *Rath*, Mit Völkerrecht gegen die NSA?, die tageszeitung, 26.8.2013, S. 12; *Kotzur*, Datenschutz als Menschenrecht, Zeitschrift für Rechtspolitik 2013, S. 216 (216). So auch *Tinnefeld*, Datenschutz 2013, Datenschutz und Datensicherheit 2013, S. 772 (774).

57 *Schaar*, Privatsphäre als Menschenrecht – Edward Snowden und die Kontrolle der Macht, Blätter für deutsche und internationale Politik 7/2014, S. 61 (64).

58 *Kotzur* (Fn. 56), S. 217.

net bereits erfasst, hätte sich die Frage gestellt, ob Art. 17 im Lichte eines neuen Protokolls einschränkend hätte ausgelegt werden müssen. Aus diesen Gründen hätte ein Zusatzprotokoll unter Umständen zu größerer Rechtsunsicherheit geführt.

Anstelle eines neuen Zusatzprotokolls brachten Deutschland und Brasilien im Herbst 2013 einen Resolutionsentwurf zum Thema in die Generalversammlung der Vereinten Nationen ein. Ursprünglich sollte dieser Entwurf auch ausdrücklich die extraterritoriale Geltung des Rechts auf Privatheit erwähnen, was von den USA jedoch abgelehnt wurde.[59] Gegen die grundsätzliche Bekräftigung dieses Rechts auch gegenüber nachrichtendienstlichen Tätigkeiten wandten sich jedoch auch die USA nicht. Die von der UN-Generalversammlung am 18. Dezember 2013 verabschiedete Resolution „The right to privacy in the digital age"[60] bekräftigt daher das Recht auf Privatleben auch im Internet. Diese im Konsens angenommene Resolution der Generalversammlung ist formal rechtlich unverbindlich.[61] Sie kann jedoch ebenso wie die Bemerkungen des Menschenrechtsausschusses als Interpretationshilfe und zur Weiterentwicklung des Art. 17 IPbpR beitragen.[62]

Die Resolution geht vom Grundsatz der funktionalen Äquivalenz des Grundrechtsschutzes im virtuellen und im realen Raum aus. Dazu heißt es: „[The General Assembly] affirms that the same rights that people have offline must also be protected online, including the right to privacy".[63] Ausdrücklich wird die massenhafte Überwachung von elektronischer Kommunikation als Menschenrechtsverletzung gekennzeichnet: „Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, (…) violate the rights to privacy and freedom of expression and may contradict the tenets of a democratic society (…)."[64] Weiterhin werden die Staaten aufgefordert, ihre bestehende Praxis zu überprüfen, und effektive Rechtsschutzmöglichkeiten bereit zu stellen.

---

59 *Schaar* (Fn. 57), S. 65; *Talmon* (Fn. 44), S. 785.

60 General Assembly, Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age, A/RES/68/167.

61 *Weichert*, Globaler Kampf um digitale Grundrechte, Kritische Justiz 2014, S. 123 (130 f.).

62 *Peters* (Fn. 31).

63 A/RES/68/167 (Fn. 60), Abs. 3.

64 A/RES/68/167 (Fn. 60), Präambelerwägung 7.

Damit zeigt sich, dass die menschenrechtlichen Verbürgungen des Rechts auf Privatheit und der Schutz der Vertraulichkeit der Kommunikation dynamisch ausgelegt und weiterentwickelt werden können.[65] Die hierfür vorgesehenen vertraglichen Institutionen und die zuständigen Organe der Vereinten Nationen haben in den vergangenen Jahren gezeigt, dass das bestehende Recht auch angesichts der Herausforderungen globaler digitaler Kommunikationstechnologien ausreichend ist und angepasst werden kann. Ob vor diesem Hintergrund neue vertragliche Initiativen sinnvoll und zielführend sind[66], ist eher fraglich. Wichtiger wäre es, dem bestehenden Recht zu größerer Durchsetzungskraft zu verhelfen.

V. Rechtliche Bewertung von Abhörmaßnahmen aus Botschaftsgebäuden

Neben den von den USA nicht bestrittenen Überwachungsmaßnahmen der NSA wurde auch der Verdacht geäußert, dass Abhörmaßnahmen aus Botschaftsgebäuden der USA durchgeführt wurden.[67] Auf derartige Aktivitäten wären neben den angeführten Menschenrechten auch die völkerrechtlichen Regeln des Diplomatenrechts anzuwenden. Diese sind überwiegend im Wiener Übereinkommen über Diplomatenrecht von 1961 (WÜD) niedergelegt, dem sowohl Deutschland als auch die USA als Vertragsparteien angehören.

Für die nachrichtendienstliche Nutzung von Botschaftsräumen oder entsprechende Tätigkeiten des diplomatischen Personals ist eine Reihe von Vorschriften einschlägig. Dazu zählt zunächst die Bindung des diplomatischen Personals an das nationale Recht nach Art. 41 Abs. 1 WÜD. So dürfen Botschaftsräume nicht zur Begehung von Straftaten benutzt werden. Weiterhin dürfen die Räume einer diplomatischen Mission nicht zu Zwecken verwendet werden, die mit den Zwecken der Mission oder völkerrechtlichen Regeln unvereinbar sind (Art. 41 Abs. 3 WÜD). Schließlich stellt Art. 3 Abs. 1 (d) WÜD, darauf ab, dass das diplomatische Personal Information mit rechtmäßigen Mitteln beschaffen muss.[68] Rechtmäßig

65 A.A. *Schmahl* (Fn. 2), S. 222, die jedoch ausschließlich auf die mangelnde gerichtliche Durchsetzbarkeit abstellt. Dazu unten VI.

66 So aber z. B. *Baum*, Wacht auf, es geht um die Menschenwürde, Datenschutz und Datensicherheit 2013, S. 583 (584).

67 *Appelbaum u.a.*, Der unheimliche Freund, Der Spiegel 44/2013, 28.10.2013, S. 20 ff.

68 *Talmon* (Fn. 3), S. 8.

meint dabei in erster Linie, dass in Einklang mit nationalem Recht gehandelt wird. Denkbar ist jedoch auch, die Vorschrift so auszulegen, dass auch Verstöße gegen das Völkerrecht und insbesondere gegen Menschenrechte eine Informationsbeschaffung rechtswidrig werden lassen.[69]

Es zeigt sich daher im Ergebnis, dass nachrichtendienstliche Tätigkeiten durch diplomatisches Personal oder aus diplomatischen Vertretungen nicht generell verboten sind. Allerdings sind Tätigkeiten, die gegen innerstaatliches Recht verstoßen, verboten und werden so zu einem Verstoß gegen das Wiener Diplomatenrecht. Daher stellen sie auch eine Völkerrechtsverletzung dar.

Allerdings stößt die praktische Durchsetzung des innerstaatlichen Rechts an die Grenzen der diplomatischen Immunität gegen Strafverfolgung nach Art. 31 Abs. 1 WÜD. Eine strafrechtliche Reaktion ist damit ausgeschlossen.[70] Vielmehr stehen einem verletzten Staat nur die begrenzten Reaktionsmöglichkeiten des Diplomatenrechts zur Verfügung. Danach kann der Empfangsstaat einen Diplomaten zur *persona non grata* erklären. Hieraus folgt die Pflicht des Entsendestaats zur Abberufung (Art. 9 Abs. 1 WÜD) und die damit verbundene Ausreise der betroffenen Person.[71] Im Übrigen regelt das Diplomatenrecht nachrichtendienstliche Tätigkeiten nur in Bezug auf die diplomatische Mission im Empfangsstaat und erfasst Überwachungen durch andere Staatsorgane nicht.

VI. Rechtsschutzfragen

Abschließend soll der Frage nachgegangen werden, mit welchen völkerrechtlichen Rechtsmitteln gegen mögliche Rechtsverletzungen durch geheimdienstliche Tätigkeiten ausländischer Nachrichtendienste vorgegangen werden könnte. Denkbar wäre zunächst eine Klage vor dem Internationalen Gerichtshof (IGH). Dieser übt jedoch keine universelle und obligatorische Gerichtsbarkeit aus, sondern ist gem. Artikel 36 des IGH-Statuts nur zuständig, wenn sich die Parteien vertraglich oder ad hoc auf

69 *Peters* (Fn. 31).

70 *Hettel/Kirschhöfer* (Fn. 9), S. 348; *Talmon* (Fn. 3), S. 8.

71 *Hettel/Kirschhöfer* (Fn. 9), S. 349; *Talmon* (Fn. 3), S. 8.

seine Zuständigkeit geeinigt haben oder wenn sich die Parteien der Gerichtsbarkeit einseitig unterworfen haben.[72]

Deutschland hat sich erst 2008 der Gerichtsbarkeit des IGH einseitig unterworfen und kann auf dieser Grundlage gegen Staaten Klage erheben, die sich ebenfalls einseitig der Gerichtsbarkeit unterworfen haben. Die USA haben ihre Unterwerfungsklausel nach dem für sie unbefriedigenden Ausgang eines Verfahrens gegen Nicaragua bereits 1984 zurückgezogen. Daher wäre eine Klage gegen die USA auf dieser Grundlage nicht möglich. Das Vereinigte Königreich hat am 31. Dezember 2014 eine einseitige Unterwerfungsklausel abgegeben, die sich auf alle Streitigkeiten bezieht, die nach dem 1. Januar 1984 entstanden sind.[73] Eine Klage gegen Großbritannien wäre insofern möglich. Diese könnte auch auf das Europäische Streitbeilegungsübereinkommen gestützt werden, an dem zahlreiche europäische Staaten beteiligt sind.[74]

Verletzungen des Wiener Diplomatenrechtsübereinkommens durch die USA könnten auch ohne Unterwerfungsklausel mit einer Klage vor dem IGH geltend gemacht werden, da sowohl die USA als auch Deutschland Vertragsparteien des Zusatzprotokolls zum WÜD betreffend der obligatorischen Streitbeilegung sind. Nach diesem Protokoll unterwerfen sich die Vertragsparteien der obligatorischen Gerichtsbarkeit des IGH für alle Streitigkeiten, die auf der Grundlage des WÜD entstehen. Allerdings wäre ein solcher Rechtsstreit auf Verletzungen des WÜD beschränkt. Verletzungen der Menschenrechte oder des Interventionsverbots könnten nur dann gerügt werden, wenn sie durch Diplomaten unter Verstoß gegen Art. 3 WÜD begangen wurden.[75] Für eine Klage Deutschlands gegen die USA vor dem Internationalen Gerichtshof, die umfassend die Tätigkeit der NSA betrifft, bliebe somit nur eine Ad-hoc-Vereinbarung übrig, die jedoch aus politischen Gründen eher unrealistisch erscheint.

Neben dem IGH wäre noch an Beschwerden zum Menschenrechtsschuss zu denken, da dieser auch Rechtsbehelfsinstanz für den IPbpR ist. Möglich wäre zunächst eine Staatenbeschwerde gem. Art. 41 IPpbR, da

---

72 *Von Arnauld* (Fn. 13), Rn. 466 ff.

73 ICJ, Declarations Recognizing the Jurisdiction of the Court as Compulsory, United Kingdom of Great Britain and Northern Ireland, 31 December 2014, http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=1&p3=3&code=GB (Abfrage vom 21.2.2015).

74 *Schmahl* (Fn. 2), S. 222.

75 *Peters* (Fn. 31).

sich sowohl die USA als auch Großbritannien diesem Mechanismus unterworfen haben. Nach dieser Vorschrift kann ein Vertragsstaat geltend machen, ein anderer Vertragsstaat komme seinen Verpflichtungen aus dem Zivilpakt nicht nach. Allerdings sieht das Verfahren eine gütliche Einigung der beteiligten Staaten unter Einbeziehung des Ausschusses vor. Eine streitige Entscheidung ist nicht möglich. Damit ist das Verfahren wenig attraktiv. Es ist in der Praxis auch noch nie genutzt worden.[76]

Neben Staatenbeschwerden kennt der Zivilpakt noch das Individualbeschwerdeverfahren nach dem Ersten Zusatzprotokoll.[77] In diesem Verfahren kann der Ausschuss auf die Beschwerde einer betroffenen Einzelperson eine Menschenrechtsverletzung feststellen. Allerdings ist das Verfahren fakultativ und setzt voraus, dass die betreffenden Staaten dem Zusatzprotokoll beigetreten sind, was weder die USA noch Großbritannien getan haben.[78] Im Übrigen würde ein Individualbeschwerdeverfahren voraussetzen, dass die beschwerdeführende Person nachweisen kann, dass in ihren Datenschutz eingegriffen wurde, was aufgrund der Natur der Sache nur selten der Fall sein dürfte.

VII. Zusammenfassung und Ausblick

Die vorstehenden Ausführungen lassen sich wie folgt zusammenfassen: Zwar besteht kein generelles völkerrechtliches Spionageverbot, jedoch ergeben sich aus dem geltenden Völkerrecht Anforderungen an konkrete nachrichtendienstliche Tätigkeiten. Allerdings setzt das allgemeine Völkerrecht ausländischen Geheimdiensten nur dann Grenzen, wenn diese die Gebietshoheit eines anderen Staates verletzten oder in dessen innere Angelegenheiten eingreifen. Abhörmaßnahmen aus diplomatischen Vertretungen dürften zudem gegen das Wiener Diplomatenrechtsübereinkommen verstoßen.

Die massenhafte Überwachung von elektronischer Kommunikation und die Speicherung von personenbezogenen Daten und Informationen, die durch die NSA und andere Geheimdienste erfolgt, werden hiervon jedoch nur eingeschränkt erfasst, da die entsprechenden Handlungen

76 *Schilling* (Fn. 50), S. 247.

77 Dazu *Schäfer/Weiß*, Das Individualbeschwerdeverfahren vor dem UN-Menschenrechtsausschuss, Zeitschrift für Europäisches Arbeits- und Sozialrecht 2004, S. 220-233.

78 *Schmahl* (Fn. 2), S. 222.

überwiegend nicht in Botschaften und nicht auf deutschem Boden stattfinden, sondern auf dem Territorium der USA.

Allerdings greifen derartige Maßnahmen in das Menschenrecht auf Privatheit und den Schutz der privaten Kommunikation ein, das global in Art. 17 IPbpR verankert ist. Diese Eingriffe können unter Berufung auf nationale Sicherheit gerechtfertigt werden, sie müssen jedoch auf einer gesetzlichen Grundlage beruhen, dem Grundsatz der Verhältnismäßigkeit genügen und gerichtlich überprüfbar sein. Die zuständigen UN-Organe haben auch angesichts der jüngsten Enthüllungen deutlich gemacht, dass der internationale Menschenrechtsschutz an moderne Kommunikationsformen angepasst werden kann und dass daher auch die Probleme, die mit Überwachungen und Informationsbeschaffungen durch Nachrichtendienste verbunden sind, menschenrechtlich bearbeitet werden können. Veränderungen des geltenden Rechts durch neue Übereinkommen oder Ergänzungen bestehender Verträge sind nicht erforderlich.

Problematisch und bislang noch nicht hinreichend geklärt ist jedoch, ob und unter welchen Umständen das Menschenrecht auf Privatheit auch extraterritorial gelten kann. Hier bedarf es noch weiterer Überlegungen und internationaler Praxis, um den Begriff der „Hoheitsgewalt" in den menschenrechtlichen Verträgen bei Eingriffen in die Freiheit im virtuellen Raum neu zu konturieren. Die gegenwärtigen technischen Grundlagen der elektronischen Kommunikation ermöglichen nämlich Eingriffe in menschenrechtlich geschützte Freiheitsräume, ohne dass ein physischer Zugriff oder eine Zugriffsmöglichkeit auf den Rechtsträger erforderlich wäre. Die damit verbundenen Herausforderungen des internationalen Menschenrechtsschutzes bedürfen in den kommenden Jahren der weiteren theoretischen Reflektion und praktischen Bearbeitung.

Letztere stößt jedoch auf internationaler Ebene schnell an die Grenzen des im Völkerrecht grundsätzlich nur schwach ausgeprägten Rechtsschutzes. Wie gezeigt sind weder zwischenstaatliche Verfahren noch Individualbeschwerden geeignet, um insbesondere gegen Maßnahmen der USA vorzugehen. In diesen Fällen sind innerstaatliche Rechtsschutzmöglichkeiten wie Gerichtsverfahren gefragt. Soweit diese völker- und menschenrechtliche Standards berücksichtigen, kann relevante Praxis entstehen. Schließlich können die Menschenrechtsorgane der UN auch ohne konkrete Rechtsstreitigkeiten durch Berichte und Stellungnahmen

zu einer Weiterentwicklung des Menschenrechts auf Privatheit gegenüber Gefährdungen im virtuellen Raum beitragen.[79]

79 *Sinha* (Fn. 1), S. 946.

Datenschutz im Steuerrecht

ROLAND ISMER[1]

I. Einleitung

Anfang dieses Jahres 2014 veröffentlichten diverse Medien Beiträge mit Titeln wie „Finanzbeamte schnüffeln in Steuerdaten ihrer Nachbarn“ (so die Süddeutsche Zeitung)[2], „Was verdient der Nachbar?“ (so die Berliner Zeitung)[3] oder schließlich „Brandenburger Ministerium bestätigt Schnüffel-Verdacht – Jeder 5. Finanzbeamte spionierte Bürger aus“ (so die BILD-Zeitung).[4] In der Tat hatte sich bei einer Überprüfung aller knapp 3300 Beschäftigten in 15 brandenburgischen Finanzämtern ergeben, dass insgesamt 727 Beamte unbefugt auf eigene Steuerdaten oder die von Verwandten zugegriffen hatten, das sind 22 Prozent aller Überprüften. In 31 Fällen hatten sich Beamte sogar unberechtigt über die Verhältnisse von Nachbarn oder Bekannten informiert. Diese illegalen Datenzugriffe erscheinen umso bedenklicher, wenn man sich vor Augen hält, dass der Steuerbürger dem Staat die Zahl seiner Kinder ebenso offenbaren muss wie seinen Familienstand, den Zustand seiner Ehe, seine Konfession, seine Parteizugehörigkeit, seine Mitgliedschaften in gemeinnützigen Vereinen sowie schwere Krankheiten, wenn die Versicherung die Kosten dafür nicht übernimmt. Im Bereich der Bildungsaufwendungen muss er seine Lebensplanung hinsichtlich seines Erwerbslebens darlegen. Mit anderen Worten: Das Steuerrecht verlangt die Offenlegung einer Vielzahl hochgradig sensibler privater Daten. Der zuverlässige Schutz solchermaßen erhobener Daten vor unberechtigter Verwendung ist Voraussetzung für das Vertrauen des Bürgers in die Finanzverwaltung und damit für sein Vertrauen in das Steuerrecht insgesamt.

---

1 Ich danke Herrn Dipl. iur. oec. Manuel Haußner für seine Hilfe bei der Erstellung und Korrektur des Manuskripts.

2 http://sz.de/1.1888462 (aufgerufen am 18.07.2014).

3 http://www.berliner-zeitung.de/brandenburg/was-verdient-der-nachbar-finanzbeamte-schnueffeln-in-steuerdaten-,10809312,26189158.html (aufgerufen am 18.07.2014).

4 http://www.bild.de/regional/berlin/finanzministerium-brandenburg/datenskandal-brandenburg-34343476.bild.html (aufgerufen am 18.07.2014).

Umgekehrt wird aber seit einiger Zeit der Ankauf illegal kopierter Daten über ausländische Bankdaten (Stichwort „Steuer-CDs“) intensiv diskutiert.[5] Derartige Geschäfte sind oftmals für den Staat sehr lukrativ. So hatte das Land Rheinland-Pfalz im April 2013 rund 4,4 Millionen Euro für eine Steuer-CD mit etwa 40.000 Datensätzen ausgegeben. Durch den Kauf des Datenträgers soll es zu Steuereinnahmen von etwa 500 Millionen Euro kommen. Dies verspricht also eine sehr gute Investition. Ob ein solcher Ankauf aber rechtmäßig ist, ist damit noch nicht gesagt; die Frage ist trotz einer Entscheidung des Bundesverfassungsgerichts (BVerfG)[6] auch noch nicht höchstrichterlich geklärt. Auf einer etwas abstrakteren Ebene geht es bei der Frage der Zulässigkeit auch um die Reichweite des Schutzes vor unbegrenzter Datenerhebung durch die Finanzverwaltung.

Von Verfassungs wegen ist der Datenschutz im Steuerrecht durch Einzelgrundrechte wie das Brief-, Post- und Fernmeldegeheimnis und den Schutz der Wohnung vor allem durch das Grundrecht auf informationelle Selbstbestimmung geboten.[7] Vor dem Hintergrund der beiden Beispiele illegaler Datenabruf durch Finanzbeamte und Ankauf von Steuer-CDs wird deutlich, dass das Datenschutzerfordernis für das Steuerrecht eine doppelte Fragestellung beinhaltet: Zunächst ist die besonders wichtige Frage nach Sicherung von Datenschutz *durch* die Finanzbehörde zu nennen; häufig wird Datenschutz im Steuerrecht mit dieser Frage gleichgesetzt, etwa wenn recht apodiktisch konstatiert wird, die Vorschrift in § 30 AO (Abgabenordnung) über das Steuergeheimnis „regelt den Datenschutz in Steuersachen“.[8] Daneben gibt es als zweite und zumeist vernachlässigte Frage diejenige nach dem Datenschutz *gegenüber* der Finanzbehörde. Der folgende Beitrag soll beiden Aspekten – also sowohl dem Datenschutz *durch* die Finanzbehörde als auch dem Datenschutz *gegenüber* der Finanzbehörde – nachgehen, wobei er sich auf das datenschutzrechtlich

5 Siehe z. B. *Gehm,* ZRP 2012, S. 223; *Habetha*, ZRP 2012, S. 223; *Kaiser*, NStZ 2011, S. 383 ff.; *Poppenhäger*, DRiZ 2013, S. 240 ff.; *Seitz,* Ubg 2014, S. 380 ff.

6 BVerfG, Beschluss vom 09.11.2010, BFH/NV 2011, S. 182-188.

7 *P. Kirchhof*, Steueranspruch und Informationseingriff, in: J. Lang (Hrsg.), Die Steuerrechtsordnung in der Diskussion, FS für Klaus Tipke, 1995, S. 27 ff.

8 *Rüsken*, in: Klein, AO, 12. Auflage, 2014, § 30 Rn. 1. Umfassend hingegen jüngst *Anzinger*, Datenschutz im Besteuerungsverfahren – Das Spannungsverhältnis zwischen Steuergerechtigkeit und informatorischer Selbstbestimmung aus steuerrechtlicher Sicht, in: Anzinger/Hamacher/Katzenbeisser (Hrsg.), Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe, 2013, S. 97 ff. Lesenswert ferner *P. Kirchhof* (Fn. 7), S. 27 ff.

besonders sensible Einkommensteuerrecht konzentrieren wird. Begonnen werden soll aber mit einer Erklärung, warum das derzeitige Einkommensteuerrecht besonders informationsintensiv ist.[9]

II. Derzeitiges Einkommensteuerrecht informationsintensiv

Die während der napoleonischen Kriege eingeführte progressive Einkommensteuer wurde im Preußen des 19. Jahrhunderts bald wieder abgeschafft. An ihre Stelle trat im Jahre 1820 zunächst eine Klassensteuer. Diese sollte – und damit sind wir wieder beim Thema Datenschutz – „zwischen einer ohne genaues Eindringen in die Vermögensverhältnisse der Pflichtigen nicht ausführbaren und deshalb immer gehässigen Einkommensteuer und einer die Gesamt-Masse aller Einwohner ohne allen Unterschied gleich treffenden Kopfsteuer die Mitte halten".[10] Die Einführung der Klassensteuer erscheint damit als eine Reaktion auf die als übermäßig empfundene Datenerhebung. Die Klassensteuer bemaß sich damit nicht nach dem genauen individuellen Einkommen.[11] Vielmehr wurden die der Steuer Unterworfenen nach äußeren Merkmalen in fünf Klassen eingeteilt. Die Steuer bestimmte sich dann entsprechend dem nach dem für die jeweilige Klasse vermuteten Einkommen. Diese grobe Art der Typisierung bedeutete, dass der Staat über wenig Informationen verfügen musste, um die Steuer zutreffend festzusetzen. In den Städten trat an ihre Stelle sogar eine Verbrauchsteuer, die Mahl- und Schlachtsteuer.

Die Klassensteuer konnte allerdings nicht hinreichend den individuellen Verhältnissen der Steuerpflichtigen Rechnung tragen, was – nicht zuletzt auch wegen der steigenden Steuerlast – zunehmend für geboten erachtet wurde. Auch die Ergänzung der Klassensteuer in den oberen Einkommensbereichen um die klassifizierte Einkommensteuer im Jahre 1851 schuf keine umfassende Abhilfe.[12] In der Folgezeit kam es dann aber zur Herausbildung einer individualisierten und synthetischen, also die Gesamtleistungsfähigkeit des Steuerpflichtigen abbildenden Einkom-

9 Grundlegend dazu *P. Kirchhof* (Fn. 7), S. 27 ff.

10 Amtsblatt der königlichen Regierung zu Magdeburg, Nr. 41, Jahrgang 1820, Klassifikationsmerkmale und allgemeine Bestimmungen, S. 296.

11 Vgl. dazu und zum Folgenden *Anzinger* (Fn. 8), S. 109 ff.; *Mathiak*, Die preußische Klassensteuer von 1820, 1999.

12 *Mathiak*, StuW 2001, S. 324 ff.

mensteuer, zunächst in Sachsen, später durch das Einkommensteuergesetz 1891 auch in Preußen. Dadurch wurde die Besteuerung an der individuellen finanziellen Leistungsfähigkeit des Steuerpflichtigen orientiert. Der Preis für die Individualisierung waren der erhöhte Informationsbedarf des Staates einerseits und das Erfordernis intensiverer Kontrollen andererseits.

Auch das gegenwärtige deutsche Einkommensteuerrecht ist am Ideal der Besteuerung nach der finanziellen Leistungsfähigkeit ausgerichtet.[13] Dieses ist zumindest teilweise von Verfassungs wegen geboten, und zwar insbesondere im Bereich der zwangsläufigen Aufwendungen, etwa für die Bestreitung des eigenen Existenzminimums des Steuerpflichtigen sowie seiner Familie. Der Gesetzgeber könnte diese Grundprinzipien daher auch dann nicht ohne Weiteres ändern, wenn er es denn wollte.

Konkretisiert wird das Leistungsfähigkeitsprinzip zum einen durch das objektive Nettoprinzip. Demnach soll der Staat nur das Einkommen der Besteuerung unterwerfen, das dem Steuerpflichtigen letztendlich zur Befriedigung persönlicher Bedürfnisse zur Verfügung steht.[14] Daher ist es erforderlich, dass der Steuerpflichtige bei der Ermittlung seiner Einkünfte Erwerbsaufwendungen abziehen kann, also Aufwendungen, die ihm im Rahmen seiner Einkunftserzielung entstehen. Terminologisch unterscheidet das deutsche Einkommensteuergesetz zwischen Betriebsausgaben und Werbungskosten. Inhaltlich besteht aber ein Gleichlauf, da beides Mal darunter Aufwendungen, die durch die steuerbare Tätigkeit veranlasst sind, verstanden werden. So kann ein Kioskbetreiber – der als Gewerbetreibender Gewinneinkünfte erzielt – die Kosten für den Getränkeeinkauf ebenso gewinnmindernd geltend machen wie die Kosten für Strom, Heizung und etwaiges Personal. Ein Lehrer kann die Kosten für den Erwerb von unterrichtsbezogener Fachliteratur, aber auch die Kosten für die Fahrt zwischen Wohnung und Schule als Werbungskosten von der Einkommensteuer absetzen. In beiden Fällen ist eine Abzugsfähigkeit aber nur gestattet, soweit sie wirklich im Zusammenhang mit der Erzielung von Einkünften stehen. Die Kosten müssen daher, soweit keine Pauschalierung wie bei der Entfernungspauschale eingreift, individualisiert angegeben werden. Um eine gerechte Besteuerung zu sichern, fordert die

13 Dazu und zum Folgenden *Birk/Desens/Tappe*, Steuerrecht, 16. Auflage, 2013, § 1 Rn. 33 ff.; Hey, in: Tipke/Lang, Steuerrecht, 21. Auflage, 2012, § 8 Rz. 42 ff.

14 *Birk/Desens/Tappe*, Steuerrecht, 16. Auflage, 2013, § 2 Rn. 189 f.; Hey, in: Tipke/Lang, Steuerrecht, 21. Auflage, 2012, § 8 Rz. 42 ff.

Finanzverwaltung zudem zumindest grundsätzlich die Vorlage von Belegen, die die Betriebsausgaben oder Werbungskosten dokumentieren. Mit anderen Worten: Zur Sicherung der gerechten Besteuerung müssen Daten offen gelegt werden.

Noch sensibler sind die persönlichen Daten, die zur Umsetzung des subjektiven Nettoprinzips offenbart werden müssen. Demnach ist es bereits verfassungsrechtlich geboten, „dass existenznotwendiger Aufwand in angemessener, realitätsgerecht bestimmter Höhe von der Einkommensteuer freigestellt wird."[15] In diesem Zusammenhang wird dem Steuerpflichtigen also gestattet, indisponiblen Lebenshaltungsaufwand steuermindernd geltend zu machen.[16] Im Einkommensteuerecht findet dieser Grundsatz an mehreren Stellen Niederschlag. Zunächst sind hier die Kinderfreibeträge zu nennen. Dies kann durchaus bedeuten, dass neben dem Mandanten selbst nur der Steuerberater und die Finanzverwaltung die genaue Zahl der Kinder kennen. Weitere besonders sensible Daten stehen im Zusammenhang mit der Abzugsfähigkeit von außergewöhnlichen Belastungen gem. § 33 EStG (Einkommensteuergesetz). Dies lässt sich an einem Beispiel verdeutlichen: Die Kosten einer künstlichen Befruchtung können bei einer Empfängnisunfähigkeit einer Frau als Krankheitskosten berücksichtigt werden. Nach neuer Rechtsprechung kommt es dabei nicht mehr auf den Familienstand an. Somit können auch zugunsten einer nicht verheirateten Frau die Kosten einer In-vitro-Fertilisation anerkannt werden.[17] Jedoch soll es bei alleinstehenden Frauen ohne feste Partnerschaft an einer Zwangslage fehlen, die für eine Berücksichtigung der Aufwendungen als außergewöhnliche Belastung erforderlich wäre.[18] Man muss also dem Finanzamt in einer solchen Situation nicht nur mitteilen, dass man empfängnisunfähig ist, sondern auch, wie fest denn die Partnerschaft ist. Und noch schlimmer: Das Finanzamt muss, wie auch immer, überprüfen, ob die Angaben stimmen.

Im Ergebnis bedeutet all dies, dass die Steuerpflichtigen nach dem derzeitigen System der an der individuellen finanziellen Leistungsfähigkeit ausgerichteten Besteuerung den Finanzbehörden umfassende Infor-

15 BVerfG, Beschluss vom 08.06.2004; BVerfGE (Entscheidungen des Bundesverfassungsgerichts) 110, S. 412-446, Rz. 67.

16 *Jakob*, Einkommensteuer, 4. Auflage, 2008, Rz. 24.

17 BFH (Bundesfinanzhof), Urteil vom 18.6.1997, BStBl II 1997, S. 805.

18 *Mellinghoff*, in: Kirchhof, EStG, 13. Auflage, 2014, § 33 Rn. 54, Stichwort „Befruchtung".

mationen zur Verfügung stellen müssen. Das Bundesverfassungsgericht hat daher schon in den 1980er Jahren zu Recht ausgeführt:

> „Die Angaben, die ein Steuerpflichtiger aufgrund des geltenden Abgabenrechts zu machen hat, ermöglichen weitreichende Einblicke in die persönlichen Verhältnisse, die persönliche Lebensführung (bis hin beispielsweise zu gesundheitlichen Gebrechen, religiösen Bindungen, Ehe- und Familienverhältnissen oder politischen Verbindungen) und in die beruflichen, betrieblichen, unternehmerischen oder sonstigen wirtschaftlichen Verhältnisse. Über ihre zeitlich kontinuierliche Erfassung, Speicherung und ständige Abrufbarkeit ermöglichen sie demjenigen, der über diese Daten verfügt, ein Wissen außerordentlichen Ausmaßes über die Betroffenen, das unter den gegenwärtigen Lebensverhältnissen in entsprechende Macht über die Betroffenen umschlagen kann."[19]

III. Datenschutz durch die Finanzbehörde

Kann eine leistungsgerechte Besteuerung daher nur erreicht werden, wenn der Steuerpflichtige seine wirtschaftlichen sowie persönlichen Daten offenbart, so bedarf es eines intensiven Datenschutzes durch die Finanzbehörde. Die von ihr erhobenen Daten müssen besonders gesichert werden. Denn mit jeder Offenlegung steigt das Risiko, dass diese Daten den verfahrensrechtlichen Bereich verlassen und zweckentfremdet gegen den Steuerpflichtigen verwendet werden können. Umgekehrt gilt: Je stärker das Vertrauen des Steuerpflichtigen in die Sicherheit seiner Daten, desto höher ist die Bereitschaft zur Offenlegung dieser.

1. Steuergeheimnis als Grundsatz

Daher hat der Gesetzgeber das Steuergeheimnis als Gegenstück zu den weitgehenden Offenbarungspflichten in der Abgabenordnung normiert.[20] Zentralnorm für den Datenschutz bzw. das Steuergeheimnis ist dabei der bereits erwähnte § 30 Abs. 1 AO: Amtsträger haben das Steuergeheimnis zu wahren; deren Verletzung ist eine Straftat nach § 355 StGB. Dieser Imperativ nimmt zwar keinen verfassungsmäßigen Rang ein, kann jedoch aufgrund des verfassungsrechtlich garantierten Anspruchs auf informati-

19 BVerfG, Beschluss vom 17.7.1984, BVerfGE 67, S. 100, 142 f.

20 *Intemann*, in: Pahlke/Koenig, Abgabenordnung, 2. Auflage, 2009, § 30 AO, Rz. 1.

onelle Selbstbestimmung gem. Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1, Art. 14 GG geboten sein.[21]

Auch wenn die Norm zunächst vermuten lässt, dass der Adressatenkreis sich nur auf Amtsträger wie z. B. Beamte und Richter (§ 7 Nr. 1 AO) beschränkt, so umfasst dieser auch die für den öffentlichen Dienst besonders Verpflichteten (siehe § 30 Abs. 3 Nr. 1 AO). Darunter fallen nicht nur Angestellte einer Behörde, sondern auch solche, die bei einem Unternehmen angestellt sind und dabei für eine Behörde Aufgaben der öffentlichen Verwaltung ausführen.[22] Der Adressatenkreis wird somit auch auf z. B. Hausmeister, Reinigungspersonal oder Mitarbeiter von Rechenzentren ausgeweitet.[23]

Diesem weiten Adressatenkreis entspricht ein ebenso weiter sachlicher Anwendungsbereich. Dieser umfasst die gesamten persönlichen, wirtschaftlichen, rechtlichen, öffentlichen und privaten Verhältnisse einer natürlichen oder juristischen Person[24], und deckt somit das gesamte Spektrum der Verhältnisse eines Steuerpflichtigen ab. Zum geschützten Personenkreis gehören dabei nicht nur die Steuerpflichtigen, sondern auch andere Personen, deren Verhältnisse einem Amtsträger in einem steuerlichen Verwaltungs- oder Gerichtsverfahren bekannt geworden sind, unerheblich davon, ob diese Personen in einem derartigen Verfahren auskunftspflichtig sind oder ihre Angaben ohne rechtliche Verpflichtung abgegeben haben.[25] Ein Amtsträger verletzt dabei das Steuergeheimnis, wenn er Daten, die ihm unter gesetzlich normierten Umständen bekanntgeworden sind, unbefugt offenbart oder verwertet (§ 30 Abs. 2 Nr. 1 und 2 AO), wobei die Relevanz dieser Daten dabei unerheblich ist.[26]

Zudem öffnet die fortschreitende elektronische Datenerhebung weitere Möglichkeiten, steuerrechtlich relevante Daten ihrem Bestimmungszweck zu entziehen. Der Gesetzgeber hat diese Problematik jedoch erkannt und gesetzlich normiert, dass bereits der unbefugte Abruf von Daten im automatisierten Verfahren, also z. B. das Kopieren von Steuerdaten, zu einer Verletzung des Steuergeheimnisses führt (§ 30 Abs. 2 Nr. 3 AO).

---

21 BVerfG, Urteil vom 17.07.1984, BStBl. II 1984, S. 634, Rn. 135.
22 AEAO (Anwendungserlass zur Abgabenordnung) zu § 30, 2.3 S. 1, 2.
23 AEAO zu § 30, 2.3 S. 4.
24 AEAO zu § 30 AO, 1.1.
25 AEAO zu § 30 AO, 1.3 S. 1 und 2.
26 AEAO zu § 30 AO, 1.1.

2. Durchbrechung des Steuergeheimnisses

Das Steuergeheimnis stellt jedoch keinen absoluten Schutz der steuerrechtlich erhobenen Daten dar. Vielmehr ermöglicht § 30 AO die Offenbarung der erlangten Kenntnisse, soweit dies zum Beispiel der Durchführung eines Verwaltungsverfahrens, eines Rechnungsprüfungsverfahrens, eines gerichtlichen Verfahrens in Steuersachen oder eines Strafverfahrens wegen einer Steuerstraftat dient oder anderweitig vom Gesetz ausdrücklich zugelassen ist. Eine solche Durchbrechung der informationellen Selbstbestimmung ist dabei auch durch das Bundesverfassungsgericht abgedeckt, unterliegt jedoch der Einschränkung des überwiegenden Interesses der Allgemeinheit. Wäre dieses durch die Wahrung des Steuergeheimnisses verletzt, so darf es unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden.[27]

Im Folgenden soll ein wenig auf den internationalen Auskunftsverkehr eingegangen werden.[28] Er kann sich auf diverse Rechtsgrundlagen stützen, die dann eine anderweitige gesetzliche Regelung im Sinne des § 30 Abs. 4 Nr. 2 AO darstellen und die Durchbrechung des Steuergeheimnisses erlauben. Insgesamt ist hier eine Zurückdrängung von Datenschutzbelangen zu verzeichnen. Insbesondere wird den Staaten versagt, sich auf innerstaatliche datenschutzrechtliche Hindernisse für die Informationsbeschaffung zu berufen. Dies bedeutet, dass etwa das weltbekannte schweizerische Bankgeheimnis erheblich an Bedeutung verliert.

Neben der unilateralen Norm des § 117 AO besteht für den internationalen Auskunftsverkehr eine Vielzahl bilateraler und multilateraler sowie supranationaler Rechtsgrundlagen. Zu nennen sind hier etwa die Europäische Amtshilferichtlinie, die Sparzinsrichtlinie, Rechtshilfeübereinkommen, aber auch die Informationsaustauschklauseln der Doppelbesteuerungsabkommen, die Regeln über die internationalen Abkommen über den Informationsaustausch in Steuersachen sowie die Regelungen im sogenannten FATCA (Foreign Account Tax Compliance Act). Die genaue Erörterung der Regelungen würde den Rahmen des Beitrags sprengen. Die folgenden Ausführungen sollen sich daher auf ein paar Bemerkungen zu den Informationsaustauschklauseln der Doppelbesteuerungsabkommen

27 BVerfG, Urteil vom 17.07.1984, BStBl. II 1984, S. 634, Rn. 136.

28 Umfassend dazu *Engelschalk*, in: Vogel/Lehner, DBA, 5. Auflage, 2008, Art. 26; Dourado, in: Reimer/Rust (Hrsg.), Double Taxation Conventions, 2014, Art. 26 (i. E.).

und den FATCA-Regelungen beschränken. Insgesamt aber lässt sich bereits an dieser Stelle festhalten, dass sich die Regelungen in einer Phase intensiver Entwicklung befinden und zunehmend ausgeweitet werden, und zwar sowohl durch Ausweitung bestehender Vorschriften als auch durch Schaffung neuer Normen.

Als erste bilaterale Grundlage sind hier die Art. 26 OECD-Musterabkommen entsprechenden Vorschriften der jeweiligen Doppelbesteuerungsabkommen zu nennen.[29] Diese sahen ursprünglich einen Auskunftsverkehr nur auf Ersuchen des anderen Vertragsstaates vor und nur soweit die Informationen zur Durchführung des Abkommens erforderlich waren. Inzwischen aber findet sich keine Beschränkung mehr auf die vom Abkommen erfassten Steuern, so dass diese Regelungen Teil eines sich herausbildenden völkervertraglichen allgemeinen Steuerverfahrensrechts darstellen. Auch besteht die Verpflichtung zum automatischen Informationsaustausch und zum sogenannten Dreiecksaustausch, bei denen der eine Vertragsstaat den anderen um Informationen ersucht, die er an Drittstaaten weitergeben will. Die übermittelten Informationen sind vertraulich und unterliegen demselben Steuergeheimnis wie innerstaatliche Steuerdaten. Begrenzt wird die Verpflichtung zum Informationsaustauch in dreierlei Hinsicht: Die übermittelten Informationen dürfen nur im Einklang mit dem innerstaatlichen Recht der beiden Staaten erhoben werden, wobei aber das Bankgeheimnis ausdrücklich nicht zu berücksichtigen ist. Auch darf der Informationsaustausch nicht gegen den Ordre-Public-Vorbehalt verstoßen. Schließlich dürfen Informationen auch dann nicht offenbart werden, wenn dadurch Wirtschafts- und Berufsgeheimnisse preisgegeben würden. Dadurch soll den Staaten die Möglichkeit eingeräumt werden, einen Missbrauch des steuerlichen Auskunftsverkehrs zum Zwecke der Wirtschaftsspionage zu verhindern.

Eine datenschutzrechtliche Besonderheit der deutschen Abkommenspraxis soll an dieser Stelle nicht unerwähnt bleiben: Es entspricht der deutschen Verhandlungsgrundlage, Informationsaustauschklauseln nur unter der Bedingung zu vereinbaren, dass die übermittelten Daten nicht in Strafverfahren verwendet werden, in denen die Todesstrafe verhängt werden kann.[30]

---

29 Zu den expansiven Tendenzen in diesem Bereich OECD, *Standard for Automatic Exchange of Financial Account Information, Common Reporting Standard,* 13. Februar 2014.

30 Vgl. Art. 25 der deutschen Verhandlungsgrundlage.

Eine für die weitere Entwicklung besonders bedeutsame Maßnahme stellt der US-amerikanische FATCA dar.[31] Nach dieser im Kern unilateralen Maßnahme müssen ausländische Finanzinstitutionen vom Beginn des Jahres 2015 an Informationen über Konten von US-amerikanischen Personen an die US-Steuerbehörden liefern, wie den Kontostand, bezogene Dividenden und Zinsen usw. Institutionen, die diese Anforderungen nicht erfüllen, werden in die steuerliche Isolation getrieben: Bedeutende Zahlungen an diese Institutionen werden einer Quellensteuer unterworfen; zur Verhinderung von Umgehungsgestaltungen gilt dies auch für Zahlungen an solche Institutionen, die über eine Institution geleistet werden, die ihre FATCA-Verpflichtungen erfüllt. FATCA würde für die betreffenden Finanzinstitutionen massive Beschränkungen bedeuten. Um diese zu vermeiden, wurde im Februar 2012 ein Abkommen zwischen den USA, Deutschland, Frankreich, Italien, Spanien und dem Vereinigten Königreich geschlossen. Danach müssen die Informationen nur an die jeweilige Heimatfinanzbehörde übertragen werden, die diese dann auf Reziprozitätsbasis übermittelt.

Diese Entwicklungen sind getrieben durch das Bestreben, Steuerhinterziehung zu bekämpfen. Indessen ist nicht zu verkennen, dass dadurch präventiv große Datenmengen übermittelt werden und damit der Datenschutz massiv zurückgedrängt wird. Dies mag unter Staaten mit vergleichbaren rechtstaatlichen Standards akzeptabel sein. Man sollte aber nicht außer Betracht lassen, dass in Diktaturen Steuerdelikte gerne zur Repression genutzt werden. Gerade die Reziprozität internationaler Verträge bedeutet aber, dass der Zugewinn an innerstaatlicher Steuergerechtigkeit durchaus durch die Förderung rechtsstaatswidriger Praktiken im anderen Staat erkauft sein kann. Im Moment ist das Pendel stark in Richtung Informationsaustausch und damit Steuergerechtigkeit geschwungen. Die genannten Datenschutzbelange sollten aber jedenfalls nicht außer Betracht gelassen werden.

IV. Datenschutz gegenüber der Finanzbehörde

Zum Datenschutz gegenüber der Finanzbehörde lässt sich ganz generell festhalten, dass es grundsätzlich keinen bedeutsamen Bereich von Informationen gibt, der der Finanzbehörde, sofern steuerlich relevant, nicht zu

31 §§ 1471-1474 of the US Internal Revenue Code.

offenbaren wäre. Mit anderen Worten: Gegenwärtig ist vor diesem Hintergrund der Datenschutz gegenüber der Finanzbehörde – anders als der starke Datenschutz durch die Finanzbehörde – nur schwach ausgeprägt.

1. E-Bilanz als Beispiel für expansive Tendenz bei der Datenerhebung

Bei der Datenerhebung ist insgesamt eine expansive Tendenz zu verzeichnen. Am deutlichsten wird dies an der sogenannten E-Bilanz: Im Zuge des „Steuerbürokratieabbaugesetzes" sind Steuerpflichtige nun verpflichtet, sowohl den Inhalt ihrer Bilanzen als auch die Gewinn- und Verlustrechnung mittels amtlich vorgeschriebenem Datensatz an die Finanzbehörden zu übermitteln. Grundsätzlich ist das Ziel der E-Bilanz zweigeteilt. Auf der einen Seite soll eine schnelle und kostensparende Übermittlung steuerrelevanter Daten ermöglicht werden.[32] Auf der anderen Seite sollen diese Daten jedoch zum Aufbau eines effektiven Risikomanagements zur Verfügung stehen, um so einen vollständigen, gleich- und gesetzmäßigen Vollzug der Steuergesetze zu ermöglichen.[33] In der Umsetzung verlangt die Finanzverwaltung jedoch weit mehr, als was aufgrund steuer- sowie handelsrechtlicher Vorgaben zu berichten wäre.[34] Somit kam es letztendlich nicht nur zur gewollten Umstellung „Elektronik statt Papier"[35], sondern auch zu einer Ausweitung der inhaltlichen Übermittlungspflicht. Diese Ausweitung macht es den Finanzbehörden nun relativ einfach, im Zusammenhang mit der elektronischen Datenübermittlung sämtliche Geschäftsvorfälle eines Unternehmens zu untersuchen[36] und tiefgreifende Einblicke in die Geschäftstätigkeit von Unternehmen zu erlangen.[37]

Dies erscheint rechtlich nicht unproblematisch, da ihr das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung entgegenstehen könnte, wonach sich eine derartige Verpflichtung zur

32 *Bergan/Schmölln/Martin,* Die elektronische Bilanz, DStR 2010, S. 1755; *Hofmeister* in: Blümich, EStG, § 5b Rz. 6 (Stand: Juni 2013).

33 *Müller*, in: Hermann/Heuer/Raupach, EStG, § 5b, Rz. 4 (Stand: Mai 2009).

34 *Dehler*, DStR-KR 2010, S. 41; *Kuntschik*, in: Kirchhof/Söhn/Mellinghoff, EStG, § 5b, Rn. B41 ff. (Stand: November 2011).

35 So Bundestag-Drucksache 16/10188, S. 13; Bundestag-Drucksache 16/10910, S. 1; Bundesrat-Drucksache 547/08, S. 14.

36 *Karla*, UbG 2012, S. 753, 756.

37 Ibid.

elektronischen Datenübertragung am Verhältnismäßigkeitsgrundsatz messen lassen muss.[38] Sofern die materiellen Rechnungslegungs- und Gewinnermittlungspflichten überschritten werden, könnte die Übermittlung darüber hinausgehender Daten gegen das Erforderlichkeitskriterium verstoßen[39] und eine exzessive Datenerlangung also verfassungsrechtlich nicht gedeckt sein.

2. Datenschutz durch Beschränkungen der Datenerhebung

Datenschutzbelange finden primär dadurch Berücksichtigung, dass nach der Abgabenordnung – wie nach anderen Verfahrensordnungen auch – bestimmte Arten der Informationserhebung beschränkt werden. So haben Angehörige eines Beteiligten nach § 101 AO ein Auskunftsverweigerungsrecht. § 102 AO schützt bestimmte Berufsgeheimnisse durch Mitwirkungsverweigerungsrechte, etwa von Geistlichen, Ärzten, Rechtsanwälten usw. Schließlich sieht § 103 AO ein Auskunftsverweigerungsrecht bei Gefahr wegen Verfolgung einer Straftat oder Ordnungswidrigkeit vor.

Viel diskutiert wird in den letzten Jahren, ob es Beschränkungen bei der Datenerhebung durch Ankauf von sogenannten Steuer-CDs gibt, wenn sich der Verkäufer die sich darauf befindlichen Daten illegal beschafft hatte. Klar ist, dass bei Zufallsfund einer solchen CD, wenn also gerade kein Ankauf stattgefunden hat, die Daten verwertbar wären. Der Ankauf wird hingegen nicht einheitlich beurteilt.

– Das Bundesverfassungsgericht hat sich in einer Entscheidung[40] aus dem Jahre 2010 über eine Verfassungsbeschwerde gegen die Verwertung von Daten aus einer Steuer-CD mit Angaben zu Kunden liechtensteinischer Bankinstitute weitgehend zurückgehalten. Es hat lediglich festgestellt, dass die angegriffene Entscheidung des Landgerichts weder als unvertretbar erscheine noch Grundrechte der Beschwerdeführer unberücksichtigt gelassen habe. Hingegen wurde die Frage, ob und inwieweit Amtsträger bei der Beschaffung der Daten nach innerstaatlichem Recht rechtswidrig oder gar strafbar gehandelt haben, ausdrücklich offen gelassen.

38 *Kuntschik* in: Kirchhof/Söhn/Mellinghoff, EStG, § 5b EstG, Rn. A39 (Stand: November 2011).

39 *Karla*, UbG 2012, S. 753, 756.

40 BFH, Beschluss vom 09.11.2010, BFH/NV 2011, S. 182-188.

- Auch das Finanzgericht (FG) Köln[41] hat im konkreten Fall ein Beweisverwertungsverbot ausdrücklich abgelehnt, jedoch nicht darüber entschieden, wie es zu beurteilen wäre, wenn die Finanzbehörde Bankangestellte angestiftet hätte, Daten auszuspähen.
- Indessen ist, wie das rheinland-pfälzische Verfassungsgericht in seinem Urteil vom Februar 2014 ausdrücklich klargestellt hat, zwischen der Datenerhebung und etwaigen Beweisverwertungsverboten zu differenzieren.[42] In verfassungsrechtlicher Hinsicht folge aus einer rechtswidrigen Beweiserhebung nicht ohne weiteres ein Verwertungsverbot, denn im Rahmen der für die Beurteilung eines fairen Verfahrens erforderlichen Gesamtschau seien nicht nur die Rechte des Beschuldigten, sondern auch die Erfordernisse einer funktionstüchtigen Strafrechtspflege in den Blick zu nehmen. Dies dürfe jedoch im Interesse des Individualrechtsschutzes nicht dazu führen, dass bereits die Beweiserhebung allein an den engeren Voraussetzungen eines Beweisverwertungsverbotes ausgerichtet wird. Die erhöhten Anforderungen an ein verfassungsrechtliches Verwertungsverbot entbänden die zuständigen Stellen nicht von ihrer Pflicht, nur in rechtskonformer Weise Beweise zu erheben. Das Gericht fügt dann hinzu, dass die rechtswidrige oder strafbare Erlangung eines Beweismittels durch eine Privatperson nur in Ausnahmefällen zu einer Unverwertbarkeit dieses Beweismittels im Strafverfahren führe. Im Hinblick auf den Ankauf von Steuerdaten-CDs sei es jedoch denkbar, dass zukünftig gleichsam mosaikartig eine Situation entstehen könnte, die es als gerechtfertigt erscheinen lässt, das Handeln eines privaten Informanten, der in rechtswidriger oder strafbarer Weise ausländische Bankdaten deutscher Steuerpflichtiger übermittelt, der staatlichen Sphäre zuzurechnen sei. Für die Frage der Zurechnung könnten auch ein gegebenenfalls erheblicher Anstieg von Ankäufen ausländischer Bankdaten und eine damit verbundene Anreizwirkung zur Beschaffung dieser Daten von Bedeutung sein.

Im Ergebnis bedeutet dies, dass wir noch keine abschließende Klarheit über die Rechtsfrage haben, ob derartige Daten erhoben werden dürfen. Es ist davon auszugehen, dass es letztlich auf eine Würdigung der Umstände des Einzelfalls ankommt, insbesondere auf die genaue Rolle der

41 FG Köln, Urteil vom 15.12.2010, EFG 2011, S. 1215.

42 VerfGH (Verfassungsgerichtshof) Rheinland-Pfalz, Urteil vom 24.02.2014 , SteuK 2014, S. 106 ff.

staatlichen Organe. Eine bloß passive Rolle ist vor diesem Hintergrund dann viel eher zulässig als eine aktiv-anstiftende. Im Übrigen sollte man sich dabei stets vor Augen halten, dass derartige Daten-CDs nicht immer zuverlässig sein müssen und auch die für eine Steuerfestsetzung oder gar Strafverfolgung erforderlichen Informationen nicht immer enthalten müssen.

3. Ansätze für ein weniger datenintensives Einkommensteuerrecht

Bereits zu Beginn des Beitrags wurde auf die Gründe hingewiesen, warum das gegenwärtige deutsche Einkommensteuerrecht so datenintensiv ist: Es besteht ein enger Zusammenhang zwischen den Anforderungen an die Steuergerechtigkeit und damit der Ausgestaltung des einfachen Steuerrechts einerseits und der Datenintensität andererseits.[43] Kaum jemand dürfte zum preußischen Klassensteuersystem zurückkehren wollen. Gleichwohl werden seit einiger Zeit vor dem Hintergrund des nur schwachen Datenschutzes bei der Datenerhebung Überlegungen angestellt, schon die Steuertatbestände im Einkommensteuerrecht so auszugestalten, dass zu ihrem Vollzug weniger sensible persönliche Daten offenbart werden müssen.[44] Dies würde zugleich die Finanzbehörden in ihrer zunehmend komplexer werdenden Aufgabe entlasten, die Daten vor unberechtigtem Fremdzugriff zu schützen.

Dieser Ansatz hilft nur bedingt im Bereich der zuvor erörterten Problematik der Hinterziehung ausländischer Einkünfte. Er ist daher kein Allheilmittel. Er könnte aber durchaus an zahlreichen Stellen zur Entschärfung der Lage beitragen. Ein erstes, durchaus gelungenes Beispiel dafür stellt die Reform der Besteuerung der Kapitalerträge durch die Unternehmenssteuerreform 2008 dar, durch die die sogenannte Abgeltungssteuer eingeführt wurde. Kapitalerträge unterliegen danach weitgehend unabhängig vom individuellen Steuersatz einem einheitlichen Steuersatz von 25 Prozent. Die Steuer wird zumeist von den Banken erhoben. Diese bedeutet zugleich, dass das Finanzamt über große Teile der im Privatvermögen erzielten Kapitalerträge, und schon gar nicht von deren Gesamtsumme, keine Kenntnis zu haben braucht. Erkauft wird dieser Vorteil

43 Dazu näher oben II.

44 Grundlegend dazu *P. Kirchhof* (Fn. 7), S. 27 ff.; *von Hammerstein*, Der verfassungsrechtliche Schutz der Privatsphäre im Steuerrecht, 1993.

allerdings, dies sollte man deutlich sehen, um den Preis einer deutlich verringerten Einzelfallgerechtigkeit, weil eine Besteuerung mit dem individuellen Steuersatz grundsätzlich ausscheidet.

Dies lässt sich an einem weiteren Beispiel verdeutlichen[45]: Nach derzeitiger Rechtslage sind die Kosten von vorweggenommenen Bildungsaufwendungen – etwa eines universitären Studiums – nur dann abzugsfähig, wenn der Steuerpflichtige einen konkreten Zusammenhang mit einer späteren Erwerbstätigkeit dartut. Derartige Pläne betreffen den beruflichen Selbstentwurf der Person. Die Pflicht zu einer Offenbarung von (Lebens-)Plänen berührt, wenn sie nicht ohnehin als Folge „steueroptimierender Anpassung" unzutreffend mitgeteilt werden, einen besonders sensiblen Bereich. Zwar liegt in steuerlichen Anreizen zur Offenbarung regelmäßig kein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Schonender – und damit der grundrechtlichen Wertung besser entsprechend – ist es jedoch, wenn der freiheitliche Staat eine „datenschutzrechtliche Generosität" zeigt und bestimmte Daten überhaupt nicht zur Kenntnis nimmt, ob sie ihm der Steuerpflichtige nun freiwillig offenbart oder nicht. Statt auf die geplante Tätigkeit abzustellen, könnte man abwarten und auf die tatsächliche Tätigkeit abstellen. Sie erfordert zum Zeitpunkt der Bildungsaufwendungen keine Erläuterung der damit verfolgten Ziele. Sie beseitigt damit die aus dem Offenbarungsanreiz folgenden Bedrohungen für das Selbstbestimmungsrecht. Sie vermeidet es daher regelmäßig, den Steuerpflichtigen überhaupt in Versuchung zu führen. Zwar ist dann immer noch eine Offenlegung des tatsächlichen Verhaltens erforderlich; diese erscheint aber weitaus weniger sensibel, weil sie nicht die Innenwelt des Selbstentwurfs, sondern die in der Sozialsphäre tatsächlich ausgeübte Tätigkeit betrifft.

4. Sonderproblem der Einbeziehung Dritter

Besondere, bisher aber wenig erörterte Probleme bereitet schließlich die Einbeziehung Dritter in das Besteuerungsverfahren, etwa der Arbeitgeber im Rahmen der Lohnsteuer oder die Banken im Rahmen der Kapitalertragsteuer. Zwar gelten die Vorschriften über den Datenschutz durch die Finanzbehörde, also insbesondere das Steuergeheimnis, auch für Dritte, da auch diese Amtsträger im Sinne des § 30 AO sind. Zumeist nicht diskutiert wird allerdings die Frage, ob der Dritte selbst wirklich Kenntnis er-

45 Dazu ausführlicher *Ismer*, Bildungsaufwand im Steuerrecht, 2005, S. 352 ff. und 500.

langen sollte über die Daten. Beispielsweise ist sicherzustellen, dass ein Arbeitgeber im Rahmen des Lohnsteuerabzugs keine Kenntnis von einer eingetragenen Lebenspartnerschaft erlangt, wenn dies einen Kündigungsgrund darstellen würde, wie dies bei kirchlichen Arbeitgebern der Fall sein kann.

V. Fazit

Das derzeitige Einkommensteuerrecht ist stark an Einzelfallgerechtigkeit orientiert. Es ist daher notwendig informationsintensiv. Dadurch besteht eine große Bedeutung der steuerlichen Datenerhebung für die Verwirklichung von Steuergerechtigkeit. Dementsprechend steht bei der Frage nach Steuerrecht und Datenschutz der Datenschutz durch die Finanzbehörde im Vordergrund, wobei insbesondere das Steuergeheimnis nach § 30 AO von zentraler Bedeutung ist. Indessen kennt dieses zahlreiche Durchbrechungen; in der letzten Zeit hat sich hier die internationale Zusammenarbeit durch Informationsaustausch intensiviert. Diese Durchbrechungen mögen der innerstaatlichen Steuergerechtigkeit dienen. Gleichwohl sollte dabei nicht übersehen werden, dass die Übermittlung von Steuerdaten an das Ausland nicht immer zu Ergebnissen führen muss, die den Wertungen des Grundgesetzes entsprechen. Ebenfalls intensiviert hat sich im Übrigen die Datenerhebung, etwa bei der E-Bilanz, so dass es zu einer Zurückdrängung des Datenschutzes gegenüber der Finanzbehörde kommt. Dem Problem sollte verstärkt dadurch entgegengetreten werden, dass die materiellen Steuergesetze eine größere Datensparsamkeit an den Tag legen durch pauschalere Regelungen und geringere Erwartungen und Anforderungen an die Einzelfallgerechtigkeit. Dann würden sich möglicherweise noch weniger Finanzbeamte für die Steuerdaten ihrer Nachbarn interessieren.

Datenschutz und Datensicherheit – mission impossible?

THOMAS KRANIG

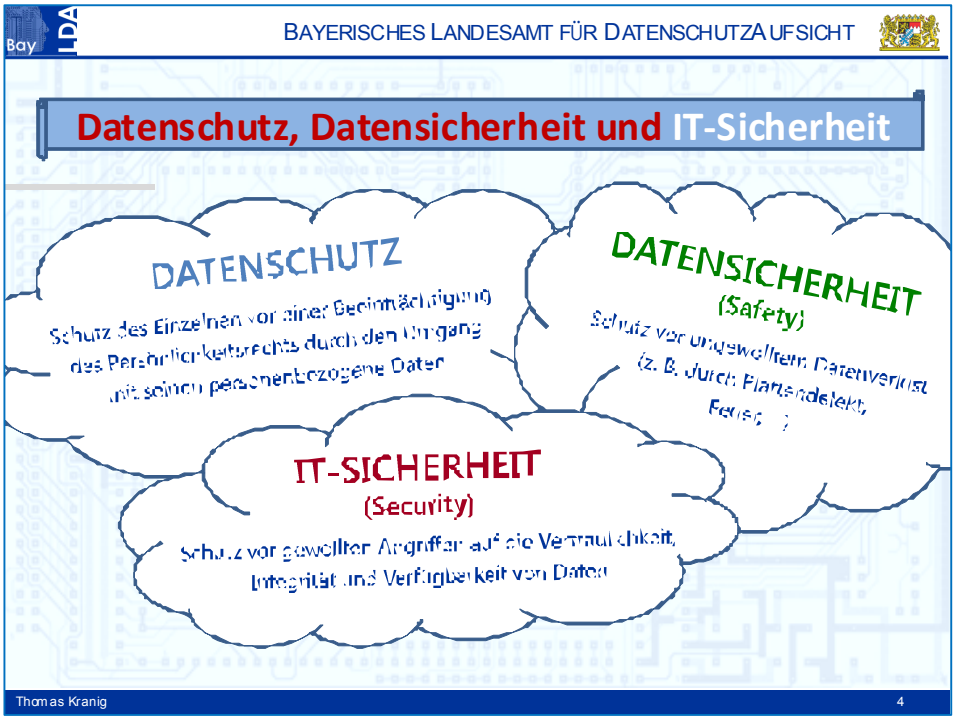
Etwa ein Jahr, nachdem Edward Snowden die Weltöffentlichkeit über die Aktivitäten unterschiedlicher Geheimdienste informierte, stellt sich die Frage, ob der Anspruch auf Datenschutz und Datensicherheit überhaupt noch Chancen hat, verwirklicht zu werden, oder ob es sich dabei um eine Frage der Unmöglichkeit (mission impossible) handelt. Dieser Frage soll aus der Sicht des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA), der einzigen Datenschutzaufsichtsbehörde in Deutschland, die ausschließlich für den nicht-öffentlichen Bereich zuständig ist, nachgegangen werden.

A. Datenschutz und Datensicherheit

Unter Datenschutz versteht man den Schutz des einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten. Dieses Ziel ergibt sich aus dem gesetzlich definierten Zweck des Bundesdatenschutzgesetzes (BDSG), den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG).

Datensicherheit beschreibt eine Sachlage, bei der Daten, personenbezogene oder auch nicht personenbezogene, unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Missbrauch bewahrt sind.

Genannt wird in diesem Zusammenhang ferner auch der Begriff der IT-Sicherheit (security), die gegeben ist, wenn die Werkzeuge der Datenverarbeitung (PC, Server, Netzwerke usw.) vor gewollten Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten geschützt sind.



1. Datenschutz

Eine einführende Darstellung des Datenschutzes in Deutschland kommt ohne einen Verweis auf die grundlegende Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 zur Volkszählung nicht aus.[1] Selbst wenn es zu diesem Zeitpunkt bereits Datenschutzgesetze gegeben hat, wurde durch die Entscheidung des Bundesverfassungsgerichts die Grundrechtsrelevanz des Datenschutzes durch Ableitung des „Rechts auf informationelle Selbstbestimmung" aus dem Grundrecht auf Schutz der Menschenwürde (Art. 1 GG) und dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 GG) wesentlich präsenter. Das Bundesverfassungsgericht hat als prägenden Inhalt dieses „neuen Datenschutzgrundrechts" geschrieben, dass „es die Befugnis des Einzelnen gewährleiste, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Wer indes nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt seien, und wer das Wissen möglicher

1 Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 65,1,43.

Kommunikationspartner nicht einigermaßen abzuschätzen vermöge, könne in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden", so das Bundesverfassungsgericht. Für die elektronische Datenverarbeitung bedeutet dies, dass der Einzelne vor der unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten bewahrt werden soll. Datenschutz ist deshalb nicht Schutz der Daten, sondern Schutz des einzelnen Menschen davor, dass andere mit seinen Daten gegen seinen Willen oder über das in bestimmten Fällen gesetzlich geregelte notwendige Maß hinaus umgehen und der Einzelne damit zu einem gläsernen Menschen wird.

Wie oben ausgeführt, soll der Einzelne davor geschützt werden, dass andere mit seinen personenbezogenen Daten unzulässig umgehen. Maßgeblich ist dabei, ob die Daten personenbezogen sind (a), ob ein datenschutzrechtlich relevantes Handeln vorliegt (b) und ob die grundlegenden Regelungen des Datenschutzes eingehalten werden (c).

a) Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), so die Definition in § 3 Abs. 1 BDSG. Maßgeblich ist insoweit auf eine Einzelperson abzustellen. Aggregierte Daten für eine Mehrzahl von Menschen sind deshalb jedenfalls dann nicht personenbezogen, wenn ein Rückschluss auf einzelne Personen nicht möglich ist. Bestimmbar sind Einzelangaben dann, wenn unter Zuhilfenahme von Informationen bei Dritten diese Einzelangaben einer konkreten Person zugeordnet werden können. Dies trifft nach Auffassung der Datenschutzaufsichtsbehörden jedenfalls für Kfz-Kennzeichen, Versicherungsnummern, Hausansichten und auch IP-Adressen[2] zu.

2 Siehe dazu Vorlagebeschluss des Bundesgerichtshofs zum Europäischen Gerichtshof (EuGH) vom 28.10.2014, Az. VI ZR 135/13, zur Klärung der Frage, ob Art. 2 Buchstabe a der EG-Datenschutz-Richtlinie dahin auszulegen ist, dass eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn lediglich ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

b) Datenschutzrechtlich relevantes Handeln

Als datenschutzrechtlich relevantes Handeln bezeichnet man den Umgang mit personenbezogenen Daten, konkret das Erheben, Verarbeiten und Nutzen dieser Daten.

Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG). Dies ist nur dann gegeben, wenn ein aktives Tun vorliegt, wie. z. B. Erfragen von Adressdaten, Filmen bestimmter Personen oder Einholen einer Auskunft bei einer Auskunftei. Eine ungewollte Entgegennahme personenbezogener Daten wie zum Beispiel das Erben einer Festplatte mit Adressdaten stellt kein Erheben dar.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Übermitteln kann dabei sowohl dadurch erfolgen, dass Daten an Dritte, z. B. durch Übergabe eines Datenträgers, weitergegeben werden als auch zur Einsicht oder zum Abruf bereit gehalten werden. Letzteres ist zum Beispiel dann der Fall, wenn man online Bonitätsdaten abrufen, im Rahmen von Homebanking Kontobewegungen einsehen kann oder in einer Arztpraxis Patientenakten für Dritte

einsehbar auf dem Empfangstresen liegen. Unter Sperren versteht man das Kennzeichnen gespeicherter personenbezogener Daten, um ihre Weiterverarbeitung oder Nutzung einzuschränken. In der Praxis geschieht dies – häufig zum Unverständnis der Betroffenen – im Zusammenhang mit Werbewidersprüchen. Adressdaten von Personen, die keine weitere Werbung empfangen wollen und deshalb widersprochen haben, werden nach wie vor gespeichert, um bei einer weiteren Werbeaktion durch Selektion der Daten sicherzustellen, dass dieser Person keine Werbung mehr zugestellt wird. Würde man in diesem Fall die Daten löschen, d. h. die gespeicherten personenbezogenen Daten unkenntlich machen, könnte die Person, die der Werbung widersprochen hat, erneut entsprechende Werbung bekommen. Datenschutzrechtlich ist es nämlich grundsätzlich zulässig, Adressdaten zu kaufen und Postwerbung zu betreiben.

Als Auffangtatbestand beim Umgang mit personenbezogenen Daten ist das Nutzen anzusehen, das jede Verwendung personenbezogener Daten darstellt, soweit es sich nicht um eine Verarbeitung im oben genannten Sinne handelt. Nutzen von Daten ist zum Beispiel gegeben, wenn ein Unternehmen die Liste seiner Kunden nach Umsätzen auswertet oder ein Arbeitgeber die Fehlzeiten seiner Beschäftigten in einer Datei zusammenfasst.

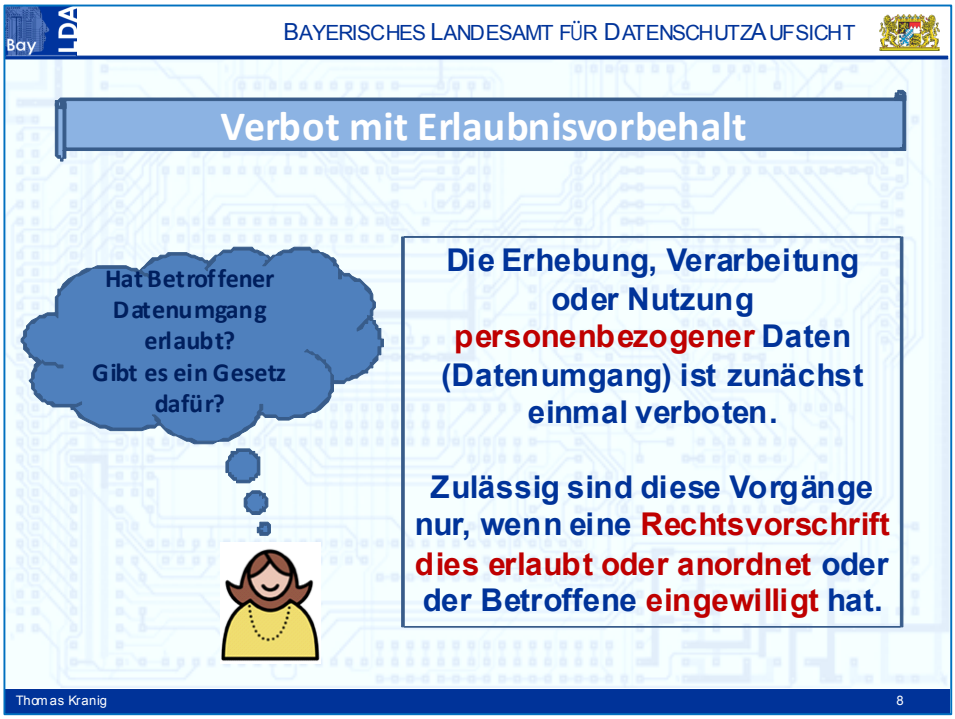
Die Differenzierung der Handlungsformen beim Umgang mit personenbezogenen Daten ist deshalb relevant, weil bestimmte Rechtsfolgen wie zum Beispiel Bußgeldandrohungen an unterschiedliche Handlungsformen anknüpfen. Bei der derzeit diskutierten europäischen Neuregelung des Datenschutzrechts in Form einer Datenschutz-Grundverordnung (siehe dazu unten) soll es diese Differenzierung nicht mehr geben, sondern nur noch den einheitlichen Begriff der Datenverarbeitung.

c) Grundsätzliche Regelungen des Datenschutzes

Für den Umgang mit personenbezogenen Daten gibt es grundsätzliche Regelungen, insbesondere das Verbot mit Erlaubnisvorbehalt (aa), das Gebot der Datenerhebung beim Betroffenen (ab), die Zweckbindung (ac), die Datensparsamkeit und Datenvermeidung (ad), die Transparenz (ae) und die Erforderlichkeit (af).

aa) Verbot mit Erlaubnisvorbehalt

§ 4 Abs. 1 BDSG bestimmt zur Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung personenbezogener Daten, dass diese nur dann rechtmäßig ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Mit anderen Worten bedeutet dies, dass jeder Umgang mit personenbezogenen Daten unzulässig ist, sofern nicht eine dieser Rechtfertigungsvoraussetzungen gegeben ist. Dass dieses oberste datenschutzrechtliche Prinzip in der Praxis von (fast) jedem von uns wiederholt verletzt wird, stellt das Prinzip als solches nicht infrage. So ist jedes „Posten" von Informationen über Dritte („bin heute mit Peter im Kino gewesen") oder Hochladen von Bildern anderer Personen auf Facebook oder YouTube ohne Einwilligung dieser Personen datenschutzrechtlich unzulässig. Auch das Herunterladen von Apps oder das Nutzen von Whats App ist jedenfalls dann unzulässig, wenn man dem App-Anbieter den Zugriff auf sämtliche Kontaktdaten erlaubt (und diese damit zum Abruf bereithält, d. h. übermittelt), ohne alle Personen, deren Anschriften, Geburtstage, Kontaktbilder, Mailadressen usw. man in seiner Kontaktliste gespeichert hat, vorher um Erlaubnis zu fragen.



bb) Gebot der Datenerhebung beim Betroffenen

Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Eine Erhebung bei dritten Personen ist nur zulässig, wenn es eine entsprechende gesetzliche Vorschrift gibt (Auskunftsersuchen durch Finanzbehörden bei Dritten), der (zulässige) Geschäftszweck eine Erhebung bei anderen Stellen erforderlich macht (Unternehmen, das einem Kunden auf Rechnung beliefern möchte, darf dessen Bonität bei der Schufa abfragen), die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und – bei allen Ausnahmeregelungen – keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Dies bedeutet, dass immer dann, wenn die Erhebung nicht bei der betroffenen Person stattfindet, generell eine Interessenabwägung stattfinden muss. Dabei ist von besonderer Bedeutung, welche Sensibilität diese Daten haben und in welchem Verwendungszusammenhang sie erhoben werden.

cc) Zweckbindung

Werden personenbezogene Daten beim Betroffenen erhoben, ist er über den Zweck der Erhebung, Verarbeitung und Nutzung dieser Daten zu informieren. An diese Aussage ist die Stelle, die mit den Daten umgehen möchte – im Datenschutzrecht als verantwortliche Stelle bezeichnet – gebunden. Möchte die verantwortliche Stelle die zu einem Zweck erhobenen Daten für einen anderen Zweck nutzen, gilt der unter aa) enthaltene Grundsatz, dass dies nur dann zulässig ist, wenn es dafür eine Rechtsvorschrift gibt, die dies erlaubt oder anordnet oder der Betroffene auch zu dem anderen Zweck seine Einwilligung erteilt hat. Relevant ist dies in der Praxis unter anderem dann, wenn man bei einem Autohändler ein Fahrzeug kauft und dafür die für den Kaufvertrag erforderlichen Daten gegebenenfalls einschließlich Bankverbindungsdaten übermittelt. Der Autohändler darf diese Daten zum Zweck der Vertragsabwicklung nutzen, sie aber nicht verwenden, um zum Beispiel Werbung zuzuschicken, die mit dem Autokauf nichts zu tun hat. Dies wäre eine Nutzung für einen anderen Zweck. Aus dem Grundsatz der Zweckbindung folgt auch, dass eine pauschale Einwilligung zur Nutzung seiner personenbezogenen Daten datenschutzrechtlich unzulässig und unwirksam wäre. Eine Einwilligung im oben genannten Autoverkäuferfall „zur Nutzung der Vertragsdaten für alle im Belieben des Autoverkäufers liegenden Zwecke“ wäre unwirksam und eine entsprechende Nutzung der Daten durch den Autohändler für sonstige Werbezwecke deshalb datenschutzrechtlich unzulässig.

dd) Datensparsamkeit und Datenvermeidung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert (§ 3a BDSG). Der beste Datenschutz ist dann gegeben, wenn personenbezogene Daten gar nicht preisgegeben werden. Diese gesetzlich fundierte Zielvorstellung findet in einer Gesellschaft, in der eine erhebliche Anzahl von Unternehmen so viele Daten wie möglich erheben und speichern wollen, um sie dann im Rahmen von Big Data auszuwerten, Profile zu bilden und für gezielte (Werbe-)Aktionen zu verwenden, häufig ihre Grenzen. Dass Firmen mit diesem Geschäftsfeld aber so großem Erfolg haben, liegt auch daran, dass die meisten von uns mit ihren Daten sehr freigebig umgehen, indem sie ihr Tagebuch auf Facebook stellen, bei jeder Verlosung Daten abgeben, für marginale Rabatte Kundenkarten nutzen, ihr Einkaufsverhalten transparent machen usw.

ee) Transparenz

Betroffene sind über die Identität der verantwortlichen Stellen, also der Stellen, die mit den personenbezogenen Daten der Betroffenen umgehen, die Zweckbestimmung der Datenverarbeitung und die Kategorien von Empfängern, soweit dies dem Betroffenen nicht erkennbar ist, zu informieren. Damit wird auch den Anforderungen des Bundesverfassungsgerichts, die es im Volkszählungsurteil aufgestellt hat, Genüge getan, dass der Betroffene darüber informiert werden soll, wer mit welchen Daten von ihm umgeht, damit er überhaupt in der Lage ist, seine Betroffenenrechte auf Auskunft, Richtigstellung, Löschung oder ähnliches geltend zu machen.

ff) Erforderlichkeit

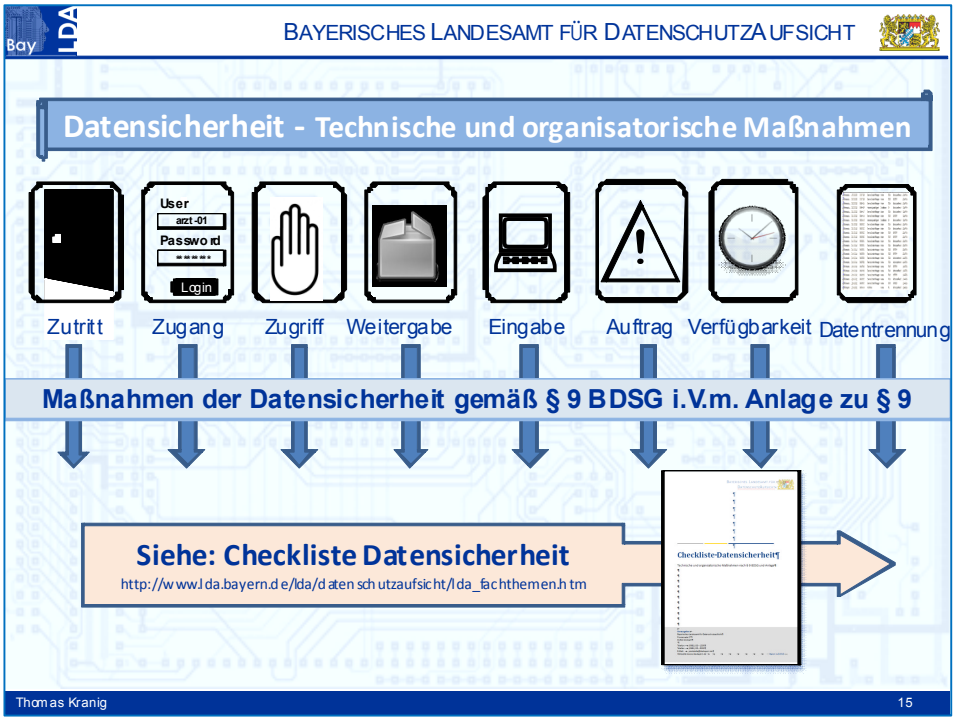
Eine Datenerhebung und -verarbeitung muss zur Zweckerreichung erforderlich sein, d. h. dem Grundsatz der Verhältnismäßigkeit entsprechen. Jeder Umgang mit personenbezogenen Daten eines Betroffenen berührt dessen Recht auf informationelle Selbstbestimmung und kann einen Eingriff in dessen Grundrechte darstellen. Ebenso wie der Staat bei jedem Grundrechtseingriff den Grundsatz der Verhältnismäßigkeit wahren, d. h.

prüfen muss, ob es zur Erreichung des angestrebten (legitimen) Zwecks kein geeigneteres, ebenso wirksames, aber weniger einschneidendes Mittel gibt, gilt dies auch im nicht-öffentlichen Bereich beim Umgang mit personenbezogenen Daten eines Dritten. Um bei dem oben genannten Beispiel des Autoverkäufers zu bleiben, mag es für den Verkäufer durchaus interessant sein zu wissen, in welchen privaten Verhältnissen der Käufer lebt, welche kulinarischen Vorlieben er hat und wohin er am liebsten mit seinem Auto fährt, um mit diesen Informationen ein verfeinertes Kundenprofil erstellen zu können. Dies könnte er nutzen, um dem Kunden noch zielgerichteter Werbung zu schicken oder ihn in Kundengesprächen deutlich verbindlicher ansprechen zu können. Diese sonstigen Informationen sind aber für die Abwicklung eines Kaufvertrages für ein Fahrzeug nicht notwendig und dürften deshalb nur mit entsprechender Einwilligung des Betroffenen gespeichert und genutzt werden.

2. Datensicherheit

Unter Datensicherheit – vielfach wird auch von Datensicherung gesprochen – wird die Gesamtheit aller technischen und organisatorischen (nicht rechtlichen) Regelungen und Maßnahmen verstanden, mit denen ein unzulässiger Umgang mit personenbezogenen Daten verhindert und die Integrität sowie Verfügbarkeit der Daten und die zu deren Verarbeitung eingesetzten technischen Einrichtungen erhalten werden sollen.[3] In § 9 BDSG und der Anlage zu § 9 sind einzelne technische und organisatorische Maßnahmen beschrieben, die insbesondere gegeben sein müssen, um Datensicherheit zu gewährleisten. Alle diese Maßnahmen stehen unter dem gesetzlichen Vorbehalt der Verhältnismäßigkeit, d. h. erforderlich sind Maßnahmen, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Abzustellen ist deshalb im Einzelfall unter anderem darauf, welche Sensibilität die Daten an sich haben (Kundenadressen oder Gesundheitsdaten), beziehungsweise in welchem Verwendungszusammenhang sie genutzt werden können.

3 Ernestus in: Simitis, Bundesdatenschutzgesetz, Rnr. 2 zu § 9.



Im Einzelnen sieht das Bundesdatenschutzgesetz folgende Schutzmaßnahmen vor:

a) Zutrittskontrolle: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, zu verwehren. Dazu könnte gehören, dass ein Serverschrank nur im Vier-Augen-Prinzip geöffnet werden darf oder es in den Unternehmen Bereiche gibt, die für Besucher tabu sind.

b) Zugangskontrolle: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. In diesem Zusammenhang könnte angeordnet werden, dass Bildschirme bei Verlassen des Arbeitsplatzes gesperrt oder Passwörter entsprechend sicher abgespeichert werden.

c) Zugriffskontrolle: Dabei ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt

werden können. Insoweit könnte man ein entsprechendes Berechtigungskonzept für Netzwerke vorsehen, aus dem sich ergibt, wer auf welche Daten zugreifen kann, oder sicherstellen, dass es keine Passwortgruppenkennungen (gleiches Passwort für alle Beschäftigen in EDV- oder Marketingabteilung) gibt oder gegebenenfalls auch USB-Anschlüsse und DVD-Laufwerke stilllegen, damit keine Daten unbefugt „hinein- oder hinauskopiert" werden können.

d) Weitergabekontrolle: Es ist sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung und während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Beispielsweise sind Datenträger nur verschlüsselt zu übergeben, oder Zugriff auf ein betriebliches Netzwerk erfolgt nur über eine gesicherte VPN-Verbindung.

e) Eingabekontrolle: Es soll nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, geändert oder entfernt worden sind. Hierzu gehört unter anderem auch die Dokumentation eines lesenden Zugriffs. So soll nachvollziehbar sein, welcher Mitarbeiter einer Bank auf welche Datensätze zugegriffen hat, auf die aus seinem Kundenbereich oder auf die von nicht in seinem Kundenbereich liegenden Prominenten (wobei in diesem Fall bei Vorliegen einer guten Konzeption der Zugriffsberechtigung im Vorhinein sichergestellt werden müsste, dass ein unbefugter Bankmitarbeiter auf die Prominentendaten gar nicht zugreifen kann). Unter dem Gesichtspunkt der Eingabekontrolle soll auch bei kritischen Datensätzen nachvollzogen werden können, wer wann welche Änderung vorgenommen hat.

f) Auftragskontrolle: Wenn personenbezogene Daten im Auftrag durch einen Anderen verarbeitet werden, darf dies nur entsprechend den Weisungen des Auftraggebers erfolgen. Wenn ein Unternehmen zum Beispiel eine Werbeagentur einschaltet und ihr die Kundendaten zur Aussendung eines Werbeschreibens übergibt, muss dieses Vertragsverhältnis detailliert dokumentiert werden. Das Unternehmen muss den Auftragnehmer gegebenenfalls auch vor Ort kontrollieren, um sicherzustellen, dass mit den personenbezogenen Daten der Adressaten datenschutzkonform umgegangen wird.

g) Verfügbarkeitskontrolle: Personenbezogene Daten sollen gegen zufällige Zerstörung oder Verlust geschützt werden. Dies kann zum Beispiel durch Einrichtung einer Notstromversorgung geschehen. Gesetzliches Ziel dieser Maßnahme ist weniger der Eigenschutz des Unternehmens als Sicherstellung der Betroffenenrechte, d. h. die Betroffenen sollen auf Dauer die Möglichkeit haben, ihr Recht auf Auskunft, Berichtigung oder Löschung ausüben zu können.

h) Zweckbindung: Dabei ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Rechtsanwälte oder Steuerberater müssen zum Beispiel Systeme vorhalten, bei denen die Daten der jeweiligen Mandanten völlig getrennt voneinander verarbeitet werden können. Bei der Entwicklung oder Fortschreibung einer Software wäre sicherzustellen, dass Test- und Produktivdaten streng getrennt bleiben.

Ergänzend dazu ist im Zusammenhang mit der Zugangs-, Zugriffs- und Weitergabekontrolle immer zu prüfen, ob und in welchem Umfang die Daten entsprechend dem Stand der Technik zu verschlüsseln sind, um z. B. unbefugtes Auslesen, Verändern oder ähnliches zu vermeiden.

Die Einhaltung dieser technisch-organisatorischen Maßnahmen (TOMs) schafft keine hundertprozentige Sicherheit – die es in keinem Fall gibt –, bietet aber eine große Gewähr, dass mit den personenbezogenen Daten auf relativ sichere Weise umgegangen wird.

Wenn Datensicherheit gegeben ist, bedeutet dies, dass Unbefugte auf die Daten keinen Zugriff haben. Datensicherheit garantiert nicht, dass mit personenbezogenen Daten auch datenschutzkonform umgegangen wird. So wäre es denkbar, dass ein gut verschlüsselter Datenträger mit Patientendaten eines Schönheitschirurgen an die Medien wandert, kein Sonstiger darauf zugreifen kann, die Daten nicht verändert werden usw. Datensicherheit wäre gewährleistet. Dies bedeutet, dass Datensicherheit gewährleistet sein kann, ohne dass der Datenschutz eingehalten ist. Im Gegensatz dazu ist Datenschutz aber nur gewährleistet, wenn auch Datensicherheit besteht. Um im Bild des obigen Beispiels zu bleiben, würde es bedeuten, dass der Datenträger mit Patientendaten in gut verschlüsselter Weise nur an jemanden übergeben werden dürfte, der datenschutzrechtlich befugt wäre, diese Daten entgegenzunehmen, d. h. zu erheben. Dies könnte zum Beispiel eine Abrechnungsstelle sein.

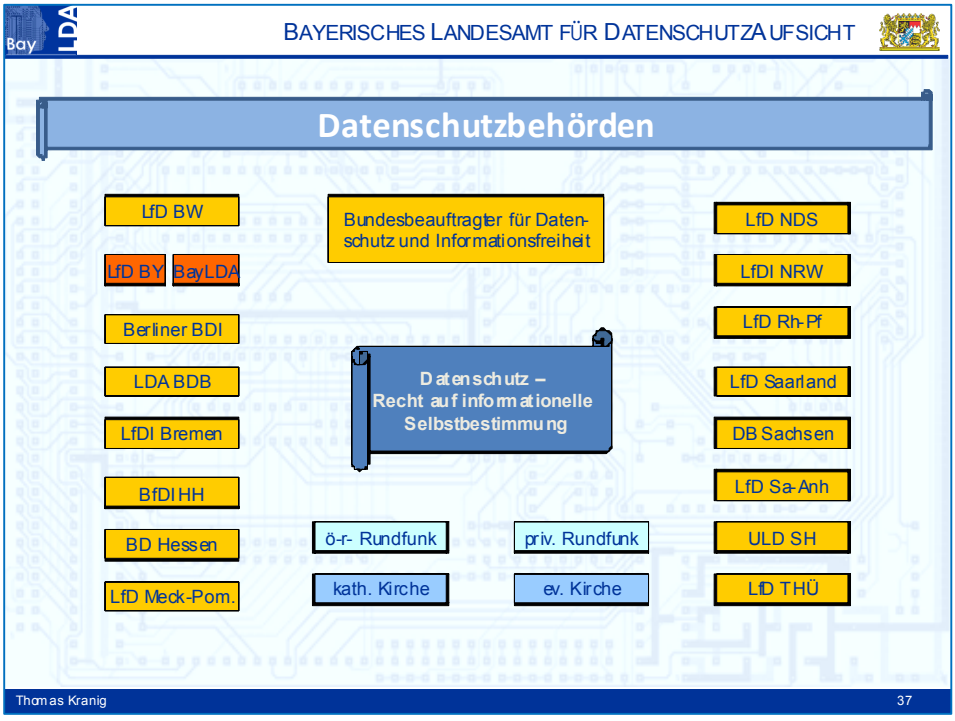
Also: Datensicherheit kann es geben ohne Datenschutz, aber Datenschutz ohne Datensicherheit gibt es nicht.

3. Datenschutz und Datensicherheit – mission impossible?

Die Verpflichtung zur Einhaltung des Datenschutzes und der Datensicherheit betrifft diejenigen Stellen, die mit personenbezogenen Daten umgehen. Die Kontrolle darüber, ob diese Stellen das Recht auf informationelle Selbstbestimmung der Betroffenen wahren, und auch die Beratung, wie diese Stellen dieses Grundrecht schützen können, obliegt den Datenschutzaufsichtsbehörden.

a. Struktur der Datenschutzbehörden

Ausgehend von den Kompetenzen, so wie sie im Grundgesetz für die Bundesrepublik Deutschland angelegt sind, gibt es auf Bundesebene die oder den Bundesbeauftragte/n für Datenschutz und Informationsfreiheit, die/der im Wesentlichen für die Einhaltung des Datenschutzes bei Bundesbehörden, Telekommunikationsunternehmen und überregional täti-



gen Krankenkassen zuständig ist. Jedes Bundesland hat ein eigenes Landesdatenschutzgesetz, in dem geregelt ist, wie die Behörden des jeweiligen Landes mit personenbezogenen Daten umzugehen haben. Entsprechend dazu gibt es in jedem Bundesland Datenschutzbehörden, die die Einhaltung dieser landesrechtlichen Vorschriften kontrollieren. Darüber hinaus sind die Datenschutzbehörden der Länder auch zuständig, den Umgang mit personenbezogenen Daten im nicht-öffentlichen Bereich, d. h. insbesondere bei Unternehmen, Verbänden, Vereinen oder freiberuflich Tätigen zu überwachen.

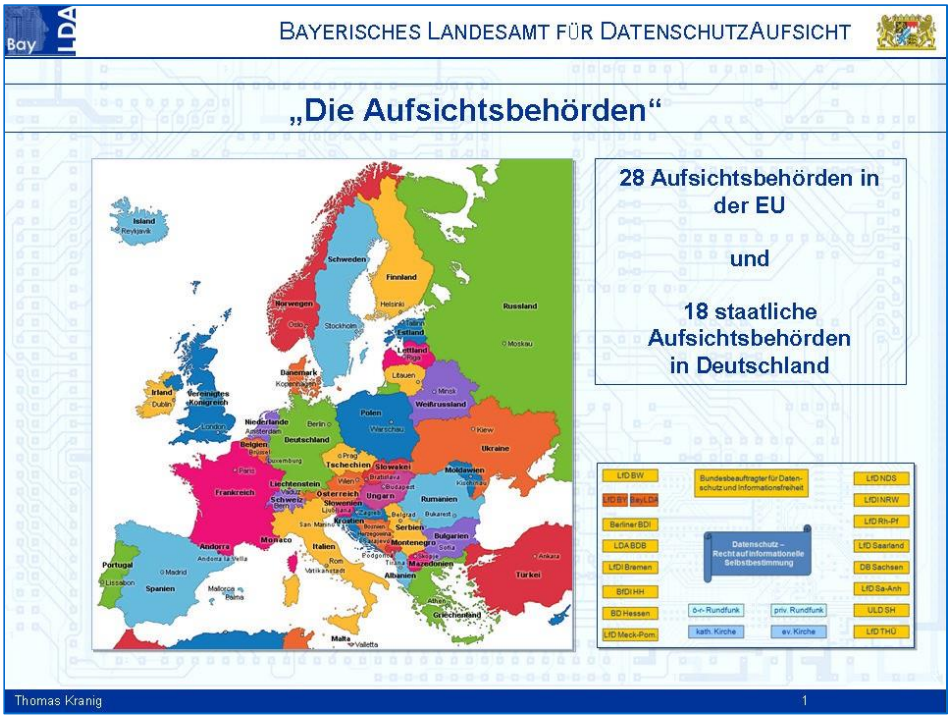
Wegen der Unabhängigkeit des Rundfunks von der staatlichen Verwaltung gibt es sowohl für den öffentlich-rechtlichen als auch den privatrechtlichen Rundfunk eigene datenschutzrechtliche Vorschriften und eigene Datenschutzbeauftragte. Dies gilt ebenso für die katholische und evangelische Kirche und deren Einrichtungen, die über eigene datenschutzrechtliche Vorschriften und Kontrollstellen für die Einhaltung der Vorschriften verfügen.

b. Unabhängigkeit der Datenschutzbehörden (Urteil des EuGH vom 9. März 2010[4])

Bereits in der Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)[5] wird in Art. 28 Abs. 1 Satz 2 bestimmt, dass die Datenschutzkontrollstellen in völliger Unabhängigkeit ihre Tätigkeit ausüben. Diese Bestimmung wurde von den deutschen Bundesländern offensichtlich zunächst nur so verstanden, dass sich dies ausschließlich auf die Datenschutzkontrolle im öffentlichen Bereich beziehe und nicht auf die Datenschutzaufsicht über nicht-öffentliche Stellen. In den meisten Bundesländern war die Datenschutzaufsicht im nicht-öffentlichen Bereich Bestandteil der allgemeinen inneren Verwaltung. Die EU-Kommission hat deshalb ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland mit dem Ziel eingeleitet, dass auch die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland völlig unabhängig ausgestaltet werden müssen. Der Europäische Gerichtshof hat mit Urteil vom 9. März 2010 der Klage stattgegeben

4 Rs. C-518/07.

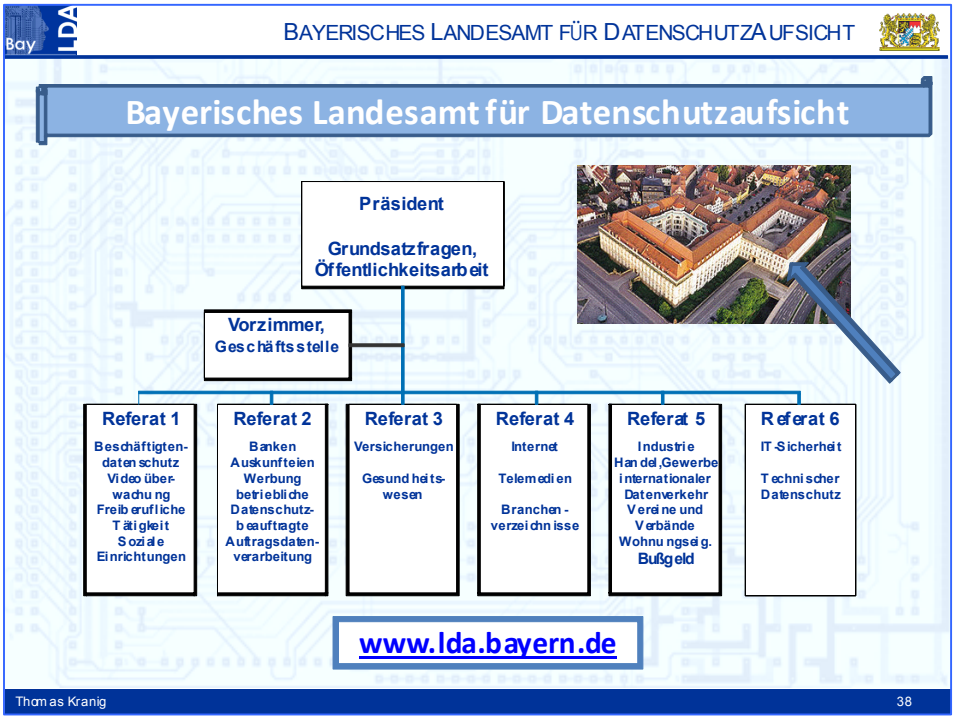
5 Amtsblatt der Europäischen Gemeinschaften vom 23.11.1995, Nr. L281/31.



und festgestellt, dass die Regelung der Datenschutzaufsicht in Deutschland in vielen Fällen nicht mit Unionsrecht vereinbar ist, da die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich der Aufsicht der Landesregierungen unterstünden und sie ihre Tätigkeit damit nicht im Sinne der Datenschutzrichtlinie in völliger Unabhängigkeit ausüben.

Die Bayerische Staatsregierung hatte auf dieses Urteil in doppelter Hinsicht reagiert. Zum einen enthielt sie sich nach Erlass des Urteils jeglicher Einflussnahme auf die Art und Weise der Datenschutzaufsicht durch das – organisatorisch nach wie vor in die Regierung von Mittelfranken eingebundene – Bayerische Landesamt für Datenschutzaufsicht. Zum anderen brachte sie zur Umsetzung des EuGH-Urteils eine Änderung des bayerischen Datenschutzgesetzes (BayDSG) auf den Weg, die vom Bayerischen Landtag mit Wirkung zum 1. August 2011 verabschiedet wurde.[6]

6 § 1 des Gesetzes zur Änderung des bayerischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 20. Juli 2011, GVBl. S. 307.



Anders als in allen übrigen Bundesländern, in denen die Zuständigkeit für die Datenschutzaufsicht im nicht-öffentlichen Bereich auf die jeweilige Kontrollstelle für den öffentlichen Bereich übertragen wurde, entschied sich der Bayerische Landtag dafür, das als Sachgebiet der Regierung von Mittelfranken bestehende Bayerische Landesamt für Datenschutzaufsicht aus der Behördenstruktur auszugliedern und zu einem unabhängigen Landesamt für Datenschutzaufsicht zu machen. Um diese Unabhängigkeit zu gewährleisten, musste unter anderem die Beleihung des TÜV Bayern e.V. mit der technischen Prüfung beendet werden. Die bisher bei der Regierung von Mittelfranken mit Datenschutz befassten Mitarbeiterinnen und Mitarbeiter wurden an das neue Landesamt versetzt. Geleitet wird dieses Landesamt von einem Präsidenten, der gemäß Art. 35 Abs. 2 BayDSG in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist. Insofern ist das Bayerische Landesamt für Datenschutzaufsicht mit seinem Zuschnitt und seiner Aufgabenstellung eine einzigartige Behörde in der Bundesrepublik Deutschland.

c. Aufgaben und Befugnisse des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA)

Das BayLDA überwacht die Einhaltung der datenschutzrechtlichen Vorschriften bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen.

aa) Aufgaben des BayLDA als Aufsichtsbehörde

Die einzelnen Aufgaben ergeben sich aus dem Bundesdatenschutzgesetz und lauten wie folgt:

- Kontrollen (§ 38 Abs. 1 Satz 1 BDSG): Das BayLDA darf, soweit das BDSG anwendbar ist, alle nicht-öffentlichen Stellen kontrollieren. Dabei müssen keine hinreichenden Anhaltspunkte für eine Datenschutzverletzung vorliegen. Selbst wenn in der Regel überwiegend anlassbezogene Kontrollen, d. h. Kontrollen aufgrund konkreter Eingaben Betroffener durchgeführt werden, führt das BayLDA, soweit es die Ressourcen zulassen, zunehmend mehr anlasslose Kontrollen durch, um eine größere Breitenwirkung der Tätigkeit zu erreichen.
- Beratung (§§ 4g, 4d, 38 Abs. 1 Satz 2 BDSG): Gesetzlich geregelt ist die Beratungsfunktion gegenüber den (betrieblichen) Datenschutzbeauftragten sowie in Zusammenhang mit Meldepflichten und Vor-Ort-Kontrollen der verantwortlichen Stellen (wie die datenverarbeitenden Stellen im Datenschutzrecht bezeichnet werden). Ferner können verantwortliche Stellen Beratungsleistungen der Aufsichtsbehörde in Anspruch nehmen. Ohne dass dies im Gesetz eine ausdrückliche Grundlage findet, werden in der Praxis in erheblichem Umfang auch Privatpersonen beraten.
- Entgegennahme von Meldungen über Datenpannen (§ 42a BDSG): Verantwortliche Stellen, bei denen besonders schützenswerte Daten abhanden gekommen sind, haben dies der Aufsichtsbehörde zu melden. Die Aufsichtsbehörde berät anschließend die verantwortliche Stelle und entscheidet gegebenenfalls über deren weiteres Vorgehen, um den Schaden zu minimieren oder zukünftige Schäden zu vermeiden.
- Prüfung der Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen (§ 38a BDSG): Berufsverbände und andere Vereinigungen können sich datenschutzrechtliche Verhaltensregelungen geben, die in einem förmlichen Verfahren der Daten-

schutzaufsichtsbehörde zur Prüfung der Vereinbarkeit mit geltendem Datenschutzrecht vorgelegt werden können.

- Genehmigung von Datenübermittlungen in Drittstaaten (§ 4c Abs. 2 BDSG): Sofern verantwortliche Stellen personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau (z. B. USA) übermitteln wollen, kann das BayLDA als Datenschutzbehörde diese Übermittlung genehmigen, wenn die entsprechenden gesetzlichen Voraussetzungen gegeben sind.
- Registerführung (§ 38 Abs. 2 Satz 1 BDSG): Das BayLDA führt das Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1 BDSG.
- Öffentlichkeitsarbeit (§ 38 Abs. 1 Satz 6 BDSG): Als verpflichtende Öffentlichkeitsarbeit hat das BayLDA spätestens alle zwei Jahre einen Tätigkeitsbericht zu veröffentlichen.

bb) Befugnisse des BayLDA als Aufsichtsbehörde

Zur Durchführung der oben genannten Aufgaben stehen dem BayLDA in seiner Funktion als Aufsichtsbehörde insbesondere folgende Befugnisse zu:

- Unterrichtung der Betroffenen und Anzeige der für den Verstoß verantwortlichen Stelle bei den zuständigen Ahndungs- und Verfolgungsbehörden (§ 38 Abs. 1 Satz 6 BDSG).
- Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel (§ 38 Abs. 5 Satz 1 BDSG).
- Untersagung der Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren bei schwerwiegenden Verstößen oder Mängeln, wenn diese entgegen der Anordnung nach § 38 Abs. 5 Satz 1 BDSG und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden (§ 38 Abs. 5 Satz 2 BDSG).
- Aufforderung zur Abberufung eines betrieblichen Datenschutzbeauftragten (§ 38 Abs. 5 Satz 3 BDSG).
- Verpflichtung der verantwortlichen Stellen zur Auskunftserteilung (§ 38 Abs. 3 BDSG), gegebenenfalls Durchsetzung mit Verwaltungszwang.

- Betreten von Grundstücken und Geschäftsräumen während der Betriebs- und Geschäftszeiten und Vornahme von Prüfungen und Besichtigungen sowie Einsichtnahme in geschäftliche Unterlagen, gespeicherte personenbezogene Daten und Datenverarbeitungsprogramme (§ 38 Abs. 4 BDSG).
- Stellung von Strafanträgen (§ 44 Abs. 2 Satz 2 BDSG).

Das BayLDA ist ferner gemäß § 11a der Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht (ZuVOWiG) zuständig für die Verfolgung und Ahndung von Zuwiderhandlungen nach § 43 BDSG sowie nach § 16 Abs. 2 Nrn. 2 bis 5 TMG.

cc) Mission impossible?

Im Freistaat Bayern gibt es etwa 600.000 verantwortliche Stellen im nichtöffentlichen Bereich, d. h. Stellen, die mit personenbezogenen Daten umgehen. Auf der anderen Seite gibt es eine Datenschutzaufsichtsbehörde mit 16 Stellen. Daraus ergibt sich ohne jede weitere Diskussion, dass eine intensive oder flächendeckende Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften in der Praxis gar nicht stattfinden kann. Wie intensiv die Kontrolle, aber natürlich auch die Beratung zur Prävention, d. h. zur Verhinderung von Datenschutzverstößen im Bund und in den Ländern jeweils stattfinden soll, ergibt sich im Wesentlichen durch die haushaltsrechtlichen Vorschriften, also die Stellenausstattung der jeweiligen Behörden.

Durch automatisierte Prüfungen in größerem Umfang und insbesondere in konzentrierter Bearbeitung aller Eingaben und Beschwerden (ca. 700 pro Jahr) und Beratung von Unternehmen (ca. 1700 pro Jahr) sowie von Bürgern (ca. 1200 pro Jahr) entfaltet das Bayerische Landesamt für Datenschutzaufsicht schon eine ganz erhebliche Breitenwirkung. Durch entsprechende Öffentlichkeitsarbeit – insbesondere den alle zwei Jahre herausgegebenen Tätigkeitsbericht und Pressemitteilungen zu einzelnen relevanten Vorgängen – ist davon auszugehen, dass den meisten Unternehmen in Bayern das Thema Datenschutz durchaus bewusst ist, selbst wenn es nicht immer ordnungsgemäß umgesetzt wird. Die „mission“ des BayLDA als Datenschutzbehörde ist deshalb sicher nicht „impossible“, selbst wenn an manchen Stellen eine intensivere Kontrolle und Ahndung von Datenschutzverstößen auch unter generalpräventiven Gesichtspunkten durchaus wünschenswert wäre.

B. Ausblick auf Europa

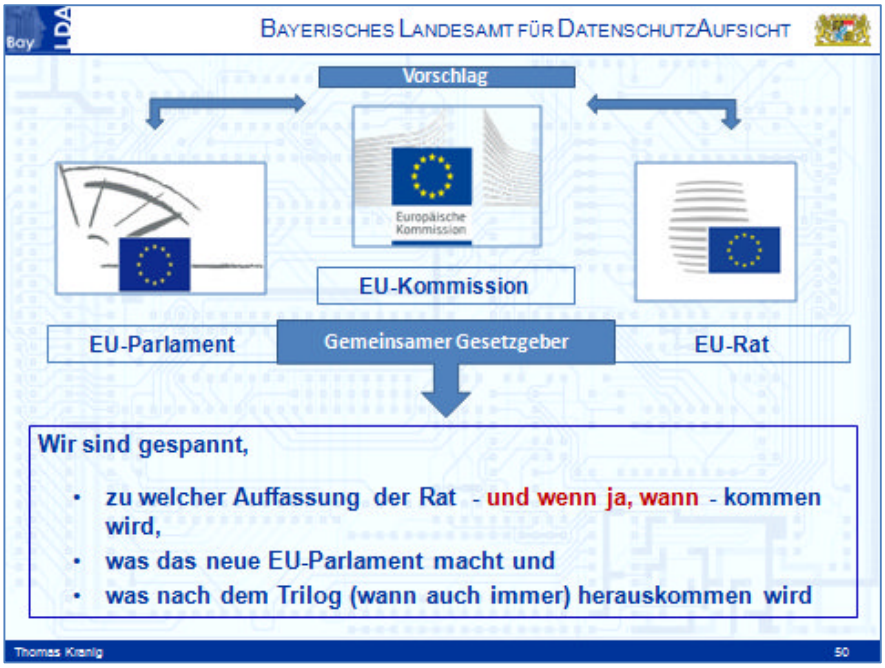
Rechtsgrundlage auf europäischer Ebene ist derzeit die Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.[7] Europäische Richtlinien richten sich an die Mitgliedstaaten und verpflichten diese zur Umsetzung in nationales Recht. Dies führt natürlich dazu, dass die Umsetzung einer Richtlinie in den jeweiligen Mitgliedstaaten unterschiedlich erfolgt. Datenschutzrechtlich muss das Gebiet der Europäischen Union deshalb als ein Fleckenteppich angesehen werden, der zwar in Form der Richtlinie ein einheitliches Grundmuster hat, aber in der Ausprägung durchaus auch erhebliche Unterschiede aufweist. Die Tatsache der fortschreitenden Globalisierung in der Wirtschaft und auch das Anwachsen der Bedeutung von Unternehmen, deren Hauptgeschäftszweck der Umgang mit personenbezogenen Daten ist, macht deutlich, dass es erforderlich ist, einen einheitlichen Rechtsstandard im Bereich der Europäischen Union zu schaffen.

Dies hatte die EU-Kommission veranlasst, am 25. Januar 2012 den Entwurf einer Verordnung (d. h. eines unmittelbar in allen Mitgliedstaaten geltenden Rechtsaktes) des Europäischen Parlaments und des Europäischen Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)[8] zur Neuregelung des Datenschutzes im Bereich der Europäischen Union vorzulegen. Dieser Entwurf, dem das Europäische Parlament am 12. März 2014 mit einigen Änderungsvorschlägen zugestimmt hat[9], sieht vor, dass es nach wie vor in den Mitgliedstaaten eine oder mehrere Aufsichtsbehörden geben kann. Es soll aber für grenzüberschreitend tätige Unternehmen eine federführende Aufsichtsbehörde im Bereich der Europäischen Union geben, die als Ansprechpartnerin dient und Entscheidungen erlässt. Die anderen Aufsichtsbehörden sollen sich in einem mit Entscheidungskompetenz ausgestatteten europäischen Datenschutzausschuss zusammenfinden, der – trotz aller Unabhängigkeit

7 ABl. 1995 Nr. L 281 S. 31.

8 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf; http://www.bundesrat.de/drs.html?id=52-12.

9 Siehe Synopse unter https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Synopse_DS_GVO_EU_Parlament_BayLDA.pdf.



der einzelnen Datenschutzbehörden – mit Mehrheit einen Beschluss fassen können soll, wie bestimmte Vorgänge datenschutzrechtlich zu bewerten und zu vollziehen sind. Selbst wenn die wesentlichen Strukturen des Datenschutzrechts auch durch die geplante Neuregelung beibehalten bleiben sollen, soll es keine unterschiedliche Behandlung mehr für den öffentlichen und nicht-öffentlichen Bereich geben. Viele Detailregelungen im deutschen Datenschutzrecht werden allgemeinen Abwägungsregelungen zum Opfer fallen. Ob das derzeit in Deutschland relativ hohe Datenschutzniveau auch in Zukunft eine entsprechende rechtliche Grundlage haben wird, bleibt abzuwarten. Geplant ist derzeit, dass im Jahr 2015 dieser europäische Rechtsakt vom Europäischen Parlament und dem Europäischen Rat verabschiedet und nach einer Übergangsphase von zwei Jahren in den Mitgliedstaaten unmittelbar gelten soll.

Dies wird zunächst unbestritten einen erheblichen Aufwand für die Gesetzgeber in Bund und Ländern mit sich bringen, um die entsprechenden datenschutzrechtlichen Vorschriften in vielen Gesetzen anzupassen. Datenschutzrecht ist eine Querschnittsmaterie, die sich in vielen Rechtsbereichen wiederfindet. Was in Zukunft wirklich gelten wird und wie sich das in der Praxis für die Betroffenen, für die Unternehmen und auch die Datenschutzbehörden anfühlen wird, weiß heute noch niemand.

Autoren- und Herausgeberverzeichnis

JOSEF FOSCHEPOTH, Professor Dr. phil., Historisches Seminar der Universität Freiburg.

Anschrift: Historisches Seminar der Universität Freiburg,
Rempartstraße 15 – KG IV, D-79085 Freiburg

E-Mail: josef.foschepoth@geschichte.uni-freiburg.de

ROLAND ISMER, Universitätsprofessor Dr. iur., MSc. Econ. (LSE), Inhaber des Lehrstuhls für Steuerrecht und Öffentliches Recht, Fachbereich Wirtschaftswissenschaften der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Anschrift: Lehrstuhl für Steuerrecht und Öffentliches Recht,
Lange Gasse 20, D-90403 Nürnberg

E-Mail: Roland.Ismer@fau.de

MARKUS KRAJEWSKI, Universitätsprofessor Dr. jur., Inhaber des Lehrstuhls für Öffentliches Recht und Völkerrecht, Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Anschrift: Lehrstuhl für Öffentliches Recht und Völkerrecht,
Schillerstraße 1, D-91054 Erlangen

E-Mail: Markus.Krajewski@fau.de

THOMAS KRANIG, Präsident des Bayerischen Landesamts für Datenschutz-Aufsicht, Ansbach.

Anschrift: Bayerisches Landesamt für DatenschutzAufsicht,
Promenade 27 (Schloss) D-91522 Ansbach

E-Mail: Thomas.Kranig@lda.bayern.de

HELMUT NEUHAUS, Universitätsprofessor (em.) Dr. phil., ehemaliger Inhaber des Lehrstuhls für Neuere Geschichte I, Department Geschichte der Philosophischen Fakultät und Fachbereich Theologie der Friedrich-Alexander-Universität Erlangen-Nürnberg, und Vorsitzender des Vorstandes der Dr. Alfred-Vinzl-Stiftung an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Anschrift: Fichtestraße 46, D-91054 Erlangen

E-Mail: Helmut.Neuhaus@fau.de

Im Rahmen der ERLANGER FORSCHUNGEN sind zuletzt erschienen:

Atzelsberger Gespräche 2002
Ethische Grenzen einer globalisierten Wirtschaft
hrsg. von Helmut Neuhaus, Erlangen 2003.
Reihe A Band 103

Atzelsberger Gespräche 2003
Der Mensch in der globalisierten Welt
hrsg. von Helmut Neuhaus, Erlangen 2004.
Reihe A Band 107

Atzelsberger Gespräche 2004
Fundamentalismus. Erscheinungsformen in Vergangenheit und Gegenwart, hrsg. von Helmut Neuhaus, Erlangen 2005.
Reihe A Band 108

Atzelsberger Gespräche 2005
Stiftungen gestern und heute. Entlastung für öffentliche Kassen?
hrsg. von Helmut Neuhaus, Erlangen 2006.
Reihe A Band 109

Atzelsberger Gespräche 2006
Die Rolle des Unternehmers in Staat und Gesellschaft
hrsg. von Helmut Neuhaus, Erlangen 2007.
Reihe A Band 113

Atzelsberger Gespräche 2007
Angst, hrsg. von Helmut Neuhaus, Erlangen 2008.
Reihe A Band 115

Atzelsberger Gespräche 2008
Gesellschaft ohne Zusammenhalt?
hrsg. von Helmut Neuhaus, Erlangen 2009.
Reihe A Band 118

Atzelsberger Gespräche 2009
60 Jahre Bundesrepublik Deutschland
hrsg. von Helmut Neuhaus, Erlangen 2010.
Reihe A Band 121

Atzelsberger Gespräche 2010
Jugendkriminalität – eine neue Herausforderung?
hrsg. von Helmut Neuhaus, Erlangen 2011.
Reihe A Band 123

Atzelsberger Gespräche 2011
Brauchen wir eine neue Ethik?
hrsg. von Helmut Neuhaus, Erlangen 2012.
Reihe A Band 126

Atzelsberger Gespräche 2012
Demokratie – Hoffnung und Krise
hrsg. von Helmut Neuhaus, Erlangen 2013.
Reihe A Band 127

Im Rahmen der FAU Forschungen ist zuletzt erschienen:

Atzelsberger Gespräche 2013
Europa zu Beginn des 21. Jahrhunderts
hrsg. von Helmut Neuhaus, Erlangen 2014.
Reihe A Band 1

Bestellungen erbeten an:
FAU University Press
Universitätsstraße 4, 91054 Erlangen
Tel.09131/85-22161 Fax 09131/85-29309
Email: ÕÎÉÖÅÒÓÉÔÙŽÐÒÅÓÓ Ί ŁÁÕ8ÄÅ

Nicht erst, aber vor allem infolge der Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden ist „Datenschutz“ zu einem großen Thema unserer Zeit geworden. Die 33. Atzelsberger Gespräche der Dr. Alfred-Vinzl-Stiftung an der Friedrich-Alexander-Universität Erlangen-Nürnberg widmeten sich ihm in Teilaspekten, indem die Referenten und übrigen Gesprächsteilnehmer zur komplizierten Gesamtproblematik in unterschiedlicher Weise Fragen aufwarfen, Antworten gaben und eine anregende Diskussion belebten. Der vorliegende Band enthält die vier Vorträge in überarbeiteter Fassung.

Der Freiburger Historiker Josef Foschepoth fragt in seinem Beitrag auf der Grundlage seines bereits in vierter Auflage vorliegenden Buches „Überwachtes Deutschland“ nach dem Zusammenhang von „Verfassung und Wirklichkeit“ am Beispiel der „Überwachung des Post- und Fernmeldeverkehrs in der Geschichte der Bundesrepublik Deutschland“. Um „Völker- und menschenrechtliche Anforderungen an Informationsbeschaffung und Datenüberwachung durch ausländische Geheimdienste“ geht es dem Erlanger Völker- und Öffentlichrechtler Markus Krajewski, während der Nürnberger Steuerrechtler Roland Ismer nicht nur vor dem Hintergrund des Ankaufs in der Schweiz illegal kopierter „Steuer CDs“ das Thema „Datenschutz im Steuerrecht“ behandelt. Schließlich stellt Thomas Kranig, der Präsident des Bayerischen Landesamts für Datenschutzaufsicht die Frage „Datenschutz und Datensicherheit – mission impossible?“ und gibt zugleich Einblicke in seine in Ansbach ansässige Behörde.

ISBN 978-3-944057-31-6
9 783944 057316

FAU UNIVERSITY PRESS 2015