ECHELON auf dem parlamentarischen Prüfstand

Alexander Dix

Dr. Alexander Dix, LL.M.

Landesbeauftragter für den Datenschutz und
für das Recht auf Akteneinsicht
Brandenburg

E-Mail: dix@lda.brandenburg.de

1 Vorbemerkung

Es ist zu begrüßen, dass der Europaausschuss des Deutschen Bundestages im Anschluss an die Diskussionen im Europäischen Parlament das Thema „ECHELON“ auf seine Tagesordnung gesetzt hat.[1] Das so bezeichnete satellitengestützte Abhörsystem, in das auch eine Station auf deutschem Boden in Bad Aibling eingebunden ist, wirft prinzipielle Fragen des Grundrechtsschutzes und insbesondere des Telekommunikationsgeheimnisses auf.[2]

Ich lege meiner rechtlichen Bewertung die Ergebnisse der sog. STOA-Berichte zu Grunde, die dem Europäischen Parlament im Januar 1998 sowie im April und Oktober 1999 vorgelegt worden sind[3]. Das Europäische Parlament hat am 5. Juni 2000 die Einsetzung eines nicht-ständigen Ausschusses beschlossen, der u.a. die Existenz des Überwachungssystems ECHELON verifizieren und die Vereinbarkeit eines derartigen Systems mit der Gesetzgebung der Europäischen Union überprüfen soll. Ohne den Ergebnissen dieses ad hoc-Ausschusses vorgreifen zu wollen, lassen jüngste Erklärungen von Vertretern der Regierung der Vereinigten Staaten indirekt den Schluss zu, dass die National Security Agency (NSA) in Zusammenarbeit mit dem britischen Geheimdienst und den Diensten anderer englisch-sprachiger Staaten (Australien, Neuseeland, Kanada) in erheblichem Umfang den weltweiten Telekommunikationsverkehr unter Einsatz von Sprachdatenbanken und Spracherkennungs-Software überwachen.

Sowohl die US-Außenministerin als auch der ehemalige Direktor des amerikanischen Geheimdienstes CIA, James Woolsey[4], haben die Existenz eines solchen Abhörsystems öffentlich bestätigt. Sie haben lediglich betont, dass damit keine Wirtschaftsspionage in dem Sinne betrieben werde, dass der amerikanische Geheimdienst Betriebs- und Geschäftsgeheimnisse ausländischer Unternehmen ausspähen und sie amerikanischen Konkurrenten zur Verfügung stellen würde. Der ehemalige CIA-Direktor hat erläutert, es würden allerdings Erkenntnisse über Bestechungsversuche europäischer Unternehmen im Zusammenhang mit großen Export-Vorhaben registriert und die beteiligten ausländischen Regierungen würden darauf hingewiesen, dass die Vereinigten Staaten solche Praktiken missbilligten.

[1] Überarbeitete Fassung der Stellungnahme d. Verf. vor dem Ausschuss für Angelegenheiten der Europäischen Union des Deutschen Bundestages am 5. Juli 2000.

[2] S. hierzu schon Endell, „Freund hört mit“ – Zur TK-Überwachung befreundeter Dienste in Deutschland, DuD 1999, S. 692 ff.

[3] STOA (Scientific and Technological Options Assessment); beide Berichte sind von Duncan Campbell verfasst und online verfügbar unter http://www.cryptome.org/stoa-atpc.htm bzw. http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf>.

Vgl. auch die weiteren STOA-Berichte „Development of Surveillance Technology and Risk of Abuse of Economic Information“ von F. Leprevost (PE 168.184/Vol 3/5/EN) und N. Bogolikos (PE 168.184/Vol 5/5)

[4] DIE ZEIT v. 30.3.2000, S.10 („Ja, liebe Freunde, wir haben Euch ausgehorcht“ – Der ehemalige CIA-Chef R. James Woolsey rechtfertigt Lauschangriffe der Amerikaner auf die Europäer: „Eure Unternehmen arbeiten mit Bestechung“)

2 Rechtliche Bewertung

2.1 Das TK-Geheimnis

Das Telekommunikationsgeheimnis wird sowohl in Art. 10 Grundgesetz (GG) als auch völkerrechtlich in einer Vielzahl von Erklärungen und Konventionen als Teil des Menschenrechts auf Schutz der Privatsphäre garantiert. Ich nenne nur die Allgemeine Erklärung zum Schutz der Menschenrechte von 1948 (Art. 12), die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten von 1950 (Art. 8) und den Internationalen Pakt über bürgerliche und politische Rechte von 1966 (Art. 17). Wie das Bundesverfassungsgericht in seinem grundlegenden Urteil zur verdachtslosen Überwachung des satellitengestützten Telekommunikationsverkehrs vom 14. Juli 1999 betont hat, ist der Schutz des Telekommunikationsgeheimnisses darauf gerichtet, *„dass die Fernmeldekommunikation von unerwünschter und unbemerkter Überwachung frei bleibt und die Grundrechtsträger unbefangen kommunizieren können. Er knüpft an das Kommunikationsmedium an und will jenen Gefahren für die Vertraulichkeit begegnen, die sich gerade aus der Verwendung dieses Mediums ergeben, das staatlichem Zugriff leichter ausgesetzt ist als die direkte Kommunikation unter Anwesenden."*[5]

Das BVerfG hat sich in dieser Entscheidung ausschließlich mit den Befugnissen des Bundesnachrichtendienstes befasst und ausdrücklich betont, dass es an dieser Stelle über geheimdienstliche Tätigkeiten, die nicht dem Gesetz zu Art. 10 GG unterliegen, nicht zu entscheiden habe. Dennoch lassen sich aus dieser Entscheidung auch wichtige Hinweise zur rechtlichen Bewertung des ECHELON-Systems ableiten. Insbesondere gilt das, was das Bundesverfassungsgericht für die verdachtslose Überwachung des nichtleitungsgebundenen Telekommunikationsverkehrs durch den Bundesnachrichtendienst ausgeführt hat, in gleicher Weise für Überwachungsmaßnahmen von ausländischen Geheimdiensten:

„Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen, hier insbesondere zur Vermeidung bestimmter Gesprächsinhalte oder Termini, führen. Dabei ist nicht nur die individuelle Beeinträchtigung einer Vielzahl einzelner Grundrechtsträger zu berücksichtigen. Vielmehr betrifft die heimliche Überwachung des Fernmeldeverkehrs auch die Kommunikation der Gesellschaft insgesamt."[6] Zur Rechtfertigung des ECHELON-Systems wird zum Teil eingewandt, es würden nicht gezielt Einzelpersonen überwacht, sondern der internationale Fernmeldeverkehr auf Grund bestimmter Suchbegriffe analysiert und gegebenenfalls aufgezeichnet. Dieser Einwand ändert jedoch nichts daran, dass die Vertraulichkeit und Sicherheit der globalen Telekommunikation durch derartige Überwachungssysteme insgesamt in Frage gestellt werden. Dementsprechend hat das Bundesverfassungsgericht die Praxis des Bundesnachrichtendienstes am Telekommunikationsgeheimnis gemessen, obwohl auch dieser sogar auf Grund einer ausdrücklichen gesetzlichen Regelung daran gehindert ist, bestimmte Telekommunikationsanschlüsse zu überwachen; auch der Bundesnachrichtendienst verwendet im Rahmen der strategischen Aufklärung Sprachdatenbanken, mit deren Hilfe Abhör- und Aufzeichnungsmaßnahmen ausgelöst werden.

Es kann daher keinem Zweifel unterliegen, dass die Überwachung des internationalen Telekommunikationsverkehrs mit Hilfe von ECHELON oder vergleichbaren Systemen in das Recht auf unbeobachtete Telekommunikation, wie es in den genannten Konventionen garantiert wird, eingreift.

2.2 NATO-Truppenstatut

Nach Auskunft der Bundesregierung (Antwort auf die Kleine Anfrage der Abgeordneten Otto u. a.[7] vom 17. April 2000 arbeitet die amerikanische Station Bad Aibling, die offenbar das weltweite Abhör-System unterstützt, auf der Grundlage des NATO-Truppenstatuts von 1951[8]. Von amerikanischer Seite ist in diesem Zusammenhang erklärt worden, das System werde zugleich im Interesse der Bündnispartner, also auch der Bundesrepublik betrieben, um z. B. illegale Waffenexporte zu verhindern. Auch der Bundesnachrichtendienst werde mit Informationen, die die Bundesrepublik betreffen, versorgt. Bekanntlich hat das Problem der illegalen Industriegüterexporte zur Herstellung biologischer Waffen nach Libyen dazu beige tragen, dass der Bundesgesetzgeber parallel hierzu mit dem Verbrechensbekämpfungsgesetz von 1994 auch die Abhörbefugnisse des Bundesnachrichtendienstes deutlich erweitert hat.

Darüber hinaus hat der ehemalige CIA-Direktor Woolsey erklärt, der amerikanische Geheimdienst registriere auch Informationen über Bestechungsversuche deutscher Unternehmen gegenüber ausländischen Regierungen[9]. Sollte dies zutreffen, so hat sich offenbar der Focus der Abhörmaßnahmen ausländischer Geheimdienste seit dem kalten Krieg verlagert. Standen zunächst sicherheitspolitische Interessen im Vordergrund, so drängt sich inzwischen der Eindruck auf, als dienten diese nur noch als Vorwand für die Verfolgung nationaler wirtschaftlicher Interessen. Der Begriff der Wirtschaftsspionage ist nicht darauf zu beschränken, dass ausgespähte Unternehmensdaten direkt anderen konkurrierenden Unternehmen zugänglich gemacht werden, selbst wenn ein solches Vorgehen dem US-Geheimdienst nach amerikanischem Recht verwehrt ist. Auch nach dem Ende des real existierenden Sozialismus können Staaten Wirtschaftsspionage betreiben. In den USA

[5] BVerfGE 100, 313 (363) m.w.N.

[6] BVerfGE 100, 313 (381) m.w.N.

[7] BT-Drs. 14/3224

[8] In Kraft getreten für die Bundesrepublik Deutschland am 1.7.1963, BGBl. II, S. 745; ergänzt durch das Zusatzabkommen vom 3.8.1959 (BGBl. 1961 II, S. 1218 ff.)

[9] S.o. FN 4

hat das Handelsministerium sich in der nationalen Diskussion der Tatsache gerühmt, in 22 Fällen deutsche Unternehmen als Wettbewerber ausgeschaltet zu haben[10].

Mit der Verlagerung des Zwecks der Abhörmaßnahmen vom Bereich der Sicherheitspolitik in den Bereich der Wirtschaftspolitik wird aber auch die Legitimationsgrundlage des NATO-Truppenstatuts verlassen. Selbst wenn die Maßnahmen noch den Zielen des Nordatlantischen Verteidigungspakts dienen würden, wären die Truppen der Vertragsparteien und ihr ziviles Gefolge verpflichtet, das Recht des Aufnahmestaates (also der Bundesrepublik Deutschland) zu achten und sich jeder mit dem Geiste dieses Abkommens nicht zu vereinbarenden Tätigkeit zu enthalten. Es ist die Pflicht des Entsendestaates, die hierfür erforderlichen Maßnahmen zu treffen[11]. Unabhängig davon sei daran erinnert, das im Zwei-Plus-Vier-Vertrag[12], dessen Abschluss sich am 12. September 2000 zum 10. Male jährt, das vereinte Deutschland die völlige Souveränität über seine inneren und äußeren Angelegenheiten zurückerhalten hat[13]. Eingriffe in diese Souveränität durch Maßnahmen ausländischer Stellen muss die Bundesrepublik nicht hinnehmen.

2.3 Europäisches Gemeinschaftsrecht

In der Unterstützung des ECHELON-Systems durch Mitgliedstaaten der Europäischen Union liegt möglicherweise auch ein Verstoß gegen europäisches Gemeinschaftsrecht. Zum einen haben sich die Mitgliedstaaten schon im Vertrag von Maastricht zur Achtung der Grundrechte nach der Europäischen Menschenrechtskonvention und den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten verpflichtet; dementsprechend wird gegenwärtig eine Europäische Charta der Grundrechte erarbeitet[14]. Die Ausspähung von Unternehmensdaten mittels Überwachung des Telekommunikationsverkehrs durch Nachrichtendienste von EG-Mitgliedstaaten wie Großbritannien dürfte auch den Zielen der Europäischen Gemeinschaft zuwiderlaufen, u. a. einen hohen Grad von Wettbewerbsfähigkeit zu fördern[15].

Auch das Europäische Sekundärrecht ist tangiert. Art. 5 der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation verpflichtet die Mitgliedstaaten, durch innerstaatliche Vorschriften die Vertraulichkeit der Telekommunikation sicher zu stellen und insbesondere das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen ohne Einwilligung der Benutzer und ohne gesetzliche Ermächtigung zu untersagen. Zwar beschränkt sich der Anwendungsbereich dieser Richtlinie auf den Binnenmarkt, aber auch dort haben die Mitgliedstaaten lediglich die Befugnis, die Vertraulichkeit der Telekommunikation zu beschränken, sofern dies für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit oder die Kriminalitätsbekämpfung notwendig ist[16]. Solche Rechtsvorschriften haben alle Mitgliedstaaten erlassen. Diese können aber von ausländischen Geheimdiensten nicht als Legitimationsgrundlage für die systematische Überwachung der Telekommunikation herangezogen werden.

Daneben verpflichtet die Allgemeine Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Daten verkehr vom 24. Oktober 1995 die Mitgliedstaaten, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewähr leisten (Art. 1 Abs. 1). Der Anwendungsbereich dieser Richtlinie ist allerdings ebenfalls auf den Binnenmarkt beschränkt. Die Mitgliedstaaten haben aber den Schutz der Privatsphäre auch bei der Zusammenarbeit in den Bereichen Inneres und Justiz zu gewährleisten (Art. K.2 EUV in der Fassung von Maastricht).

Jeder Mitgliedstaat kann den Europäischen Gerichtshof anrufen, wenn er der Auffassung ist, dass ein anderer Mitgliedstaat (z. B. durch die Beteiligung am ECHELON-System) gegen eine Verpflichtung aus dem Vertrag zur Gründung der Europäischen Gemeinschaft verstoßen hat[17].

2.4 Innerstaatliches Recht

Ob die verdeckte Telekommunikationsüberwachung, die dem ECHELON-System zu ge schrieben wird, nach dem jeweiligen innerstaatlichen Recht der Staaten, die dieses System betreiben, zulässig wäre, müsste im Einzelnen rechtsvergleichend untersucht werden; im Rahmen dieser Stellungnahme ist dies nicht zu leisten. Es kann aber festgehalten werden, dass eine systematische Überwachung des Fernmeldeverkehrs durch ausländische Nachrichtendienste im Geltungsbereich des Grundgesetzes weder mit dessen Art. 10 noch mit den Vorschriften des G10-Gesetzes vereinbar ist. Auch der Straftatbestand der Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) dürfte objektiv verwirklicht sein.

Zwar sind nur deutsche Staatsorgane unmittelbar zur Einhaltung deutscher Rechtsvorschriften, insbesondere des Telekommunikationsgeheimnisses, verpflichtet und können zur Einhaltung dieser Verpflichtung von deutschen Gerichten angehalten werden. Die Bundesregierung könnte aber von Verfassungswegen verpflichtet sein, entweder den Betrieb der Abhörstation in Bad Aibling ganz zu unterbinden oder zumindest nur unter bestimmten Bedingungen weiterhin zuzulassen. Die Bundesregierung hat in ihrer Antwort auf die Kleine Anfrage des Abgeordneten Otto und der Fraktion der FDP[18] er-

[10] So D. Campbell in seiner Stellungnahme gegenüber dem Bundestagsausschuss für Angelegenheiten der Europäischen Union am 5.7.2000

[11] Art. II NATO-Truppenstatut; s. dazu im einzelnen Endell, DuD 1999, S.694 f.

[12] BGBl. 1990 II, S. 1318

[13] Art. 7 Abs. 2

[14] Art. F Abs. 2 und K.2 des Europäischen Unionsvertrages in der Fassung von Maastricht; der Entwurf der Grundrechtscharta ist u.a. veröffentlicht in Neue Justiz 2000, S. 472 ff.

[15] Art. 2 EGV i.d.F. von Amsterdam

[16] Art. 14 Abs. 1 der Telekommunikations-Datenschutzrichtlinie (97/66/EG)

[17] Art. 227 EGV i.d.F. von Amsterdam

[18] BT-Drs. 14/3224

klärt, das Parlamentarische Kontrollgremium sei über die Einschätzung informiert worden, die sachverständige Stellen innerhalb der Bundesregierung zu den STOA-Berichten des Europäischen Parlamentes abgegeben hätten. Dies und die bloße Wiedergabe der Versicherung ausländischer Nachrichtendienste oder Regierungen, es werde nicht gegen gesetzliche Bestimmungen verstoßen, genügt allerdings nicht, um eine gleichwertige Kontrolldichte zu erreichen, wie sie das deutsche Recht zur Kontrolle der Geheimdienste in der Bundesrepublik vorsieht. Auch der Umstand, dass der amerikanische und der britische Geheimdienst in ihren Entsendestaaten einer wie auch immer gearteten parlamentarischen Kontrolle unterliegen, macht eine wirksame Kontrolle in der Bundesrepublik nicht überflüssig.

Ich halte es deshalb nicht für ausgeschlossen, dass die Bundesregierung vom Bundesverfassungsgericht auf eine entsprechende Klage hin dazu verpflichtet werden könnte, in Verhandlungen mit den ausländischen Regierungen, die diese Form der Telekommunikationsüberwachung betreiben, für einen effektiveren Schutz des Fernmeldegeheimnisses der Bundesbürgerinnen und Bundesbürger zu sorgen. Ich erinnere daran, dass das Bundesverfassungsgericht in seinem Urteil vom Juli 1999 z.B. die Pflichten des Bundesnachrichtendienstes zur Benachrichtigung der Betroffenen nach Abschluss der Überwachungsmaßnahme erweitert hat[19]. Schon jetzt müsste der Bundesnachrichtendienst bei der Verwertung von Informationen ausländischer Geheimdienste denselben Benachrichtigungspflichten unterliegen wie bei Maßnahmen, die er selbst nach dem G 10 durchführt.

3 Konsequenzen

a) Die grundsätzliche Frage, ob die Tätigkeit von Geheimdiensten überhaupt rechtlich zu regulieren ist, hat die Bundesrepublik Deutschland positiv beantwortet. Geheimdienste sind Teil der staatlichen (vollziehenden) Gewalt, die der Grundrechtsbindung nach Art. 1 Abs. 3 des Grundgesetzes unterliegen. Die Gesetze zur Tätigkeit des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes wie auch das Gesetz zu Art. 10 Grundgesetz enthalten detaillierte Regelungen über die Befugnisse der Dienste, in Grundrechte einzugreifen. Ausländische Geheimdienste, die für Mitgliedstaaten des Nordatlantikpaktes in der Bundesrepublik tätig sind, haben diese verfassungsrechtlichen und einfachgesetzlichen Bestimmungen zu achten (Art. II NATO-Truppenstatut).

b) Unabhängig von den rechtlichen Rahmenbedingungen sollte die Bundesregierungssichere Verschlüsselungstechnik sowohl den Unternehmen als auch den Bürgerinnen und Bürgern zur Verfügung stellen und verstärkt in diesem Bereich öffentliche Fördermittel einsetzen. Mit ihren Eckpunkten für eine Kryptopolitik hat die Bundesregierung in dieser Richtung im vergangenen Jahr ein wichtiges Signal gesetzt. Sichere Verschlüsselungsverfahren sollten als kostenlose Standardleistung von allen Telekommunikationsunternehmen angeboten werden. Auch nach Ablauf der von der Bundesregierung vorgesehenen zweijährigen Evaluationsfrist sollte die Bundesrepublik nicht dem britischen Beispiel folgen und den fruchtlosen Versuch unternehmen, den privaten Einsatz von Verschlüsselungssoftware einzuschränken.

c) Das Beispiel ECHELON weist zugleich auf die wachsende Bedeutung der Informationsfreiheit hin. Die ersten Hinweise auf das ECHELON-System wurden in den Vereinigten Staaten auf der Grundlage des Freedom of Information Act publik gemacht. Es ist zu hoffen, dass auch in Großbritannien, wo ein entsprechendes Gesetz dem Unterhaus bereits vorliegt, und in der Bundesrepublik, wo die Bundesregierung ihre Absicht erklärt hat, ein Informationszugangsgesetz für die Bundesverwaltung auf den Weg zu bringen, die Transparenz entscheidend verbessert wird. Geheimschutz und Verwaltungstransparenz müssen sich nicht diametral gegenüberstehen. Ein Mindestmaß an Transparenz der Methoden und Verfahren (ohne sofortige Offenlegung der gesammelten Informationen) ist unabdingbare Voraussetzung für jede rechtsstaatliche und demokratische Kontrolle.

[19] BVerfGE 100, 313, 398 f.