Anforderung einer Stellungnahme durch den Untersuchungsausschuss des Bundestags zur Untersuchung der Enthüllungen von Edward Snowden über die Internet- und Telekommunikationsüberwachung: Die öffentliche Debatte im Vereinigten Königreich

Von Ben Hayes am 1. Juli 2015

I EINLEITUNG

1. Ich bin wissenschaftlicher Mitarbeiter des Amsterdamer Transnational Institute und freischaffender Forscher und Berater zu Sicherheits- und Menschenrechtsthemen im Vereinigten Königreich.[1] Ich wurde gebeten, dem Ausschuss eine „detaillierte Beschreibung der Debatte zu vermitteln, die sich seit den Enthüllungen Edward Snowdens im parlamentarischen, öffentlichen und akademischen Bereich im Vereinigten Königreich über Themen zu den Aktivitäten der eigenen Nachrichtendienste des Vereinigten Königreichs, der parlamentarischen Kontrolle dieser Aktivitäten sowie zum Schutz der Privatsphäre abspielt; dazu gehören auch ein Überblick über wichtige Dokumente, Stellungnahmen sowie sonstige Informationen, die von der Regierung, dem Parlament, Nichtregierungsorganisationen oder anderen Akteuren in diesem Bereich veröffentlicht wurden."

2. Zu diesem Zweck enthält meine Stellungnahme sechs wesentliche Abschnitte, die sich mit folgenden Sachverhalten befassen: (i) Die Position der britischen Regierung zu den Enthüllungen Snowdens (Absatz 3-22); (ii) begleitende Entwicklungen, die zur Erweiterung der Überwachungsdebatte beigetragen haben (Absatz 23-42); (iii) Untersuchungen und Prüfungen durch das britische Parlament und andere wichtige Akteure (Absatz 43-68); (iv) richterliche Überprüfung und Überwachungsreform (Absatz 69-84); (v) zivilgesellschaftliche Kampagnen (Absatz 85-100); und (vi) die Bedeutung dieser Informationen für Deutschland (Absatz 101-107).

II DIE POSITION DER BRITISCHEN REGIERUNG ZU DEN SNOWDEN-ENTHÜLLUNGEN

3. Dieser Abschnitt erklärt die Reaktion der [britischen] Regierung zu den Enthüllungen von Snowden und ihre Position zu wichtigen politischen Überlegungen. Es ist zweckdienlich, die öffentliche Debatte von diesem Ausgangspunkt aus zu analysieren, da die Debatte nach einer kurzen Phase einer „Schadensbegrenzung" zunehmend durch die öffentlichen Stellungnahmen der Regierung und ihrer Nachrichtendienste geprägt war.

Vorläufige Feststellungen

4. Es wurde argumentiert, die britische Regierung habe es geschafft, die öffentliche Debatte zu prägen und einzuschränken, weil die Regierung von weitestgehend „folgsamen" Mainstream-Medien profitieren konnte, die außer in wenigen Ausnahmefällen relativ wenig über die Snowden-Enthüllungen und die Probleme berichteten, die sich im Hinblick auf die Grundrechte und demokratische Regierungsführung im Zusammenhang mit den Enthüllungen ergaben. Dr. Arne Hintz von der *School of Journalism, Media and Cultural Studies* an der Universität Cardiff (Wales) weist beispielsweise darauf hin, dass „Zeitungen wie die Times and der Daily Telegraph den Guardian [der die ersten Snowden-Enthüllungen veröffentlichte] beschuldigten, die Sicherheit des Landes zu gefährden, und sich damit in den Dienst der Regierung und der Spionageagenturen stellten. Die Berichterstattung durch den Rundfunk- und Fernsehsender BBC war allenfalls dürftig. Während die Enthüllung vom 20. September [2013], dass der britische Geheimdienst den belgischen Telekommunikationsanbieter Belgacom angezapft hatte, um

[1] In den vergangenen 20 Jahren war ich auch Angestellter der Londoner Bürgerrechtsorganisation Statewatch, des European Center for Constitutional and Human Rights in Berlin, der Human Security Collective in Den Haag, des Friedensforschungsinstituts Oslo, sowie im Bereich Trilaterale Forschung und Beratung tätig. Meine Forschungs- und Beratungsarbeiten habe ich u. a. für die Europäische Kommission, für das Europäische Parlament, die Vereinten Nationen, die International Federation of Journalists, das Internationale Komitee vom Roten Kreuz sowie für die Open Society Foundations durchgeführt.

EU-Institutionen auszuspionieren, für großes Interesse außerhalb des Vereinigten Königreichs sorgte, hat die BBC die Meldung überhaupt nicht gebracht."[2]

5. Mehrere Regierungen in Folge haben auch stillschweigende Unterstützung durch die großen Oppositionsparteien erfahren, deren Kritik allenfalls gedämpft war – auch hier gab es allerdings bedeutende Ausnahmen aus den eigenen Reihen – und hinzu kamen die wesentlichen Ergebnisse des UK Investigatory Powers Tribunal (IPT), des juristischen Organs im Vereinigten Königreich, das Beschwerden von Mitgliedern der Öffentlichkeit über die Überwachung anhört und darüber befindet); generell hat dieses Tribunal die Rechtmäßigkeit der Politik und Praxis der Government Communications Headquarters (GCHQ) bestätigt (s. Abs. 70-72). Das Auftreten des „Islamischen Staates" und die Entscheidung hunderter britischer Staatsbürger, sich dieser Gruppierung anzuschließen, in Verbindung mit einer gnadenlosen Fokussierung der Regierung und der Medien auf „Radikalisierung", insbesondere „Online-Radikalisierung", wurde auch herangezogen, um eine Überwachungsgewalt durch die Regierung zu rechtfertigen und öffentliche Unterstützung dafür zu erlangen (s. Abs. 40-42).

6. Während sich zahlreiche Menschen außerhalb des Vereinigten Königreichs für die offensichtliche Inkongruenz zwischen der Größenordnung dessen, was Snowden enthüllt hat, und einem wahrgenommenen Mangel an öffentlicher und politischer Besorgnis seitens der britischen Bevölkerung interessierten – zumindest im Vergleich zu Ländern wie Deutschland – würde ich sagen, dass die politische Kultur des Respekts gegenüber den Sicherheitsapparaten im Vereinigten Königreich vielleicht einmalig ist unter Staaten mit vergleichbaren demokratischen und rechtlichen Traditionen. Die Auswirkungen der Snowden-Enthüllungen sollte man meiner Meinung nach nicht im luftleeren Raum sehen, sondern im Zusammenhang mit der größtenteils völligen Straffreiheit für rechtswidriges Verhalten des Sicherheitsdienstes in vielen Jahrzehnten britischer Operationen zur Zerschlagung von Aufständen in den ehemaligen Kolonien des Landes, gegen die irischen Nationalisten im Norden Irlands sowie in der jüngeren Vergangenheit beim sogenannten „Krieg gegen den Terror". Ich teile die Meinung von Sir Stephen Sedley, ehemaliger Richter am Berufungsgericht, der im Zuge der Snowden-Enthüllungen kommentierte, dass der Sicherheitsapparat „in der Lage ist, ein Maß an Macht gegenüber den anderen Gliedern des Staates auszuüben, das einer Autonomie nahekommt: Durchsetzung von Gesetzen, die seine eigenen Interessen gegenüber den Rechten Einzelner priorisieren, Beherrschung der Entscheidungsfindung der Exekutive und Blockierung von Gerichtsverfahren seiner Gegner und Agieren fast ohne jegliche Kontrolle durch die Öffentlichkeit."[3]

7. Es scheint auch, als ob wenige Mitglieder der Exekutive sich überhaupt über den Umfang der Überwachung durch die britischen Nachrichtendienste[4] vor den Snowden-Enthüllungen bewusst waren. Nach Angaben von Chris Huhne, Minister zur Zeit der Enthüllungen, wurde dem Kabinett seinerzeit „nichts über Tempora von GCHQ oder Prism der NSA oder über ihre außergewöhnliche Fähigkeit, persönliche E-Mails, Sprachkontakte, Aktivitäten in sozialen Netzen und sogar Internetsuchen abzufangen und zu speichern, gesagt. Huhne, der auch Mitglied des UK National Security Council war, in dem Minister und Leiter der Geheim- und Sicherheitsdienste, GCHQ und das Militär eine Rolle spielen, sagte ferner: „Ich weiß nicht, ob der Premierminister oder Außenminister (der für die Aufsicht des GCHQ zuständig ist) unterrichtet wurde, der NSC jedenfalls nicht."[5] Dass es dem politischen System des Vereinigten Königreichs an Kapazitäten und Erfahrung mangelt, um seine mächtigsten und geheimsten staatlichen

---

"Snowden, the Media and Surveillance: Looking back at the Leak of the Year", 18. Dezember 2013, hier verfügbar: http://www.iomec.co.uk/blog/snowden-the-media-and-surveillance-looking-back-at-the-leak-of-the-vear/.

[3] "Beware Kite-Flyers", Londoner Bücherrezension, 12. September 2013, verfügbar unter: http://www.lrb.co.uk/v35/n17/stephen-sedlev/beware-kite-flvers.

[4] Der Begriff "Nachrichtendienste" bezieht sich auf den Security Service (MI5), den Secret Intelligence Service (MI6) und die Government Communications Headquarters (den Signalaufklärungsdienst des Vereinigten Königreichs – GCHQ).

[5] "Prism und Tempora: Dem Kabinett wurde nichts über die Exzesse des Überwachungsstaates berichtet." Guardian, 6. Oktober 2013, verfügbar unter: http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet- surveillance-state.

Dienste mehr als nur formal zur Rechenschaft zu ziehen, sollte man nach meiner Meinung nicht mit Apathie oder Indifferenz seitens der gesamten Bevölkerung gleichsetzen.

„Weder bestätigen noch dementieren"

8. Seit Jahrzehnten schon gilt die Formulierung „Weder bestätigen noch dementieren" (Neither confirm nor deny, NCND) als Standardantwort von Ministern und Beamten bei Fragen zu den Aktivitäten der britischen Nachrichtendienste. Die bloße Existenz des GCHQ wurde erst Anfang der 1980er Jahre amtlich bestätigt, und bis zur Verabschiedung des Gesetzes über die Nachrichtendienste (Intelligence Services Act) von 1994 wurde die Agentur rechtlich nicht reguliert. NCND wurde routinemäßig als Antwort auf Fragen verwendet, die durch von Snowden veröffentlichte Dokumente aufgeworfen wurden, und wird oftmals von pauschalen Zusicherungen begleitet, dass die Nachrichtendienste stets im Rahmen des Gesetzes handeln. Diese Haltung scheint Zweifel in der Öffentlichkeit über die Schwere und den Wahrheitsgehalt der Enthüllungen Snowdens hervorzurufen.

9. Der Regierung gelang es sogar, ihre *„neither confirm nor deny"*-Haltung im Laufe der Verhandlungen vor dem Investigatory Powers Tribunal (IPT) im Hinblick auf ihr „Tempora-Programm" aufrechtzuerhalten, sodass das IPT nur darüber befinden konnte, ob Tempora aus hypothetischer Sicht nach britischem Recht zulässig wäre (s. Abs. 70-72).

10. Die Regierung musste jedoch einiges einräumen und die Existenz mehrerer von Snowden enthüllter Praktiken bestätigen. Im Hinblick auf den Datenaustausch mit ausländischen Nachrichtendiensten, einschließlich der National Security Agency (NSA) der USA, sah sich die Regierung gezwungen, dem IPT gegenüber offenzulegen, dass die Vereinbarungen extrem großzügig sind (s. Abs. 90-91). Die britischen Nachrichtendienste können große Mengen an „nichtanalysierten" Massendaten ohne Gerichtsbeschluss erhalten und abrufen, wenn es „nicht technisch machbar" für sie wäre, die Informationen selbst zu beschaffen. Dieses „ausländische Nachrichtenmaterial" – dazu gehören sowohl die Metadaten als auch die Inhalte von Kommunikationen – könnte dann in einer großen durchsuchbaren Datenbank bis zu zwei Jahre lang gespeichert werden; der Zugriff auf diese Datenbank würde nicht dem Regulation of Investigatory Powers Act 2000 (RIPA), dem Überwachungsgesetz des Vereinigten Königreichs, unterliegen.[6]

11. Ein weiteres wichtiges Eingeständnis erfolgte bei der Zeugenaussage von Charles Farr, dem Director General des Office for Security and Counter Terrorism im britischen Innenministerium. Farr bestätigte, dass alle über webbasierte Plattformen außerhalb des Vereinigten Königreichs übermittelten Kommunikationen nach dem RIPA als „externe Kommunikationen" behandelt werden. Das ist wichtig, weil der RIPA eine rechtliche Unterscheidung zwischen „internen" und „externen" Kommunikationen vorschreibt. Im Endeffekt verlangt der RIPA, dass die interne Überwachung „gezielt" (wenn auch „locker") zu erfolgen hat, während die externe Überwachung wahllos oder „pauschal"[7] durchgeführt werden kann. Diese Bestimmungen sind mit denen der USA vergleichbar, die Sicherheitsvorkehrungen im Hinblick auf interne Kommunikationen von US-Bürgern vorsehen, gleichzeitig aber eine rasterartige ausländische Überwachung nach Section 702 des Foreign Intelligence Surveillance Act erlauben. Viel wichtiger jedoch ist, dass die Zeugenaussage Farrs bestätigte, dass aufgrund der Regierungsdefinition dessen, was eine „externe Kommunikation" darstellt, fast alle über soziale Netzwerke wie Facebook und Twitter oder über Google-Suchmasken, YouTube, Webmail-Dienste wie Gmail, Yahoo und Hotmail

---

[6] "Secret policy reveals GCHQ can get warrantless access to bulk NSA data", Liberty, 29. Oktober 2014, verfügbar unter: https://www.liberty-human-rights.org.uk/news/press-releases/secret-policy-reveals-gchq-can-get- warrant-less-access-bulk-nsa-data.

[7] Interne Kommunikationen können nur mit einer Anordnung des Innenministers nach Paragraph 8(1) abgefangen werden, die bei Verdacht auf eine strafbare Handlung ergeht und den Gegenstand der Intervention oder eine Reihe von Voraussetzungen angeben muss. Das Abfangen externer Kommunikationen bedarf einer Anordnung nach Paragraph 8(4), die nur ergehen kann, wenn der Innenminister die Überwachung für erforderlich hält, und die keine Angabe zu dem beabsichtigten Ziel der Intervention erfordert.

verschickte Kommunikationen sowie E-Mails an nicht-britische Staatsbürger im Ausland oder von ihnen generell nach dem weniger strengen externen Standard im RIPA überwacht werden können.[8] Daher würde das GCHQ eine Nachricht, die über eine dieser Kommunikationsplattformen im Vereinigten Königreich verschickt wird, selbst wenn sowohl ihr Absender als auch der Empfänger sich im Vereinigten Königreich befindet, als „externe Kommunikation" ansehen (weil nicht im Vereinigten Königreich stationierte Webserver zur Übermittlung der Nachricht zum Einsatz kamen). Nach Maßgabe eines Ministerialzertifikats mit breit gefassten Begründungen ist es den britischen Nachrichtendiensten gestattet, alle diese „externen Kommunikationen" zu lesen, anzuhören und anzusehen. Die einzige offensichtliche Einschränkung ist, dass sie dieses Material nicht mithilfe von „Selektoren" (Schlüsselwörter oder Begriffe) durchsuchen können, die sich konkret auf britische Staatsbürger oder Einwohner beziehen. Die Aussage Farrs stellte ein nie zuvor dagewesenes Eingeständnis dar, dass britische Staatsbürger, die über angeblich private Kanäle miteinander kommunizieren, legitime gesetzliche Ziele für eine Überwachung ohne entsprechende Anordnung sind. Bei der unabhängigen Überprüfung von Terrorismusgesetzen im Vereinigten Königreich wurde kürzlich vorgeschlagen, dieses „Schlupfloch" zu schließen (s. Abs. 62-68).

12. Farr bestätigte die Existenz der U.S.-Programme „Prism" und „Upstream Collection", weil sie „ausdrücklich durch die Exekutive der U.S.-Regierung eingestanden worden" war.[9] Genauso bestätigte er, dass das GCHQ Informationen aus dem Prism-Programm bezogen hat, weil dies vom Intelligence and Security Committee im Juli 2013 bestätigt worden war (s. Abs. 45). Es hat jedoch keine weiteren Eingeständnisse oder Offenlegungen im Hinblick auf das Verhältnis des Vereinigten Königreichs zu den USA, die sog. „Fünf Augen" oder sonstige Nachrichtendienstpartnerschaften gegeben, obwohl die Regierung so weit gegangen ist, die Behauptung, dass Vereinbarungen dieser Art zur Umgehung des inländischen Rechtsschutzes verwendet werden, zu dementieren. Der Innenminister sagte: „Es wird behauptet, unsere Agenturen stützten sich auf ihre Pendants in Übersee – namentlich in den Vereinigten Staaten – die ihnen abgefangene Kommunikationen illegal zur Verfügung zu stellen. Das ist einfach nicht wahr."[10]

13. Die Regierung hat ihre Politik, weder zu bestätigen noch zu dementieren, im Hinblick auf wiederholte Behauptungen, dass das GCHQ juristische Personen im Ausland wie Belgacom und Gemalto „gehackt" hat, aufrechterhalten; im Februar 2015 hat sie allerdings die weltweiten „Hacking"-Fähigkeiten der Nachrichtendienste erstmals bei einem Beratungsgespräch im Innenministerium über den Entwurf eines Verhaltenskodex zum Einsatz von Fangschaltungen und dergleichen effektiv bestätigt. Die Veröffentlichung des Kodex war eindeutig eine Antwort auf schwebende Verfahren am IPT und nicht auf einen übergeordneten Wunsch nach größerer Transparenz seitens der Regierung (s. Abs. 75-80) zurückzuführen. Der für den Kodex verantwortliche Minister merkte an, dass „es Grenzen gibt für das, was in der Öffentlichkeit über diese Arbeit gesagt werden kann", und stellte fest: "Die Fähigkeiten, die Kommunikationen eines Verdächtigen zu lesen oder anzuhören oder in seinen Rechner einzugreifen, sind die wichtigsten, sensibelsten und am strengsten kontrollierten Befugnisse, die dem Staat zur Verfügung stehen".[11]
14. Über alle anderen Fragen zu den Snowden-Enthüllungen, darunter auch die Teilnahme von britischen Nachrichtendiensten an „Drohnenattacken" und „außergerichtlichen Hinrichtungen" (s. Abs. 38-39), hat die Regierung ihre traditionelle Politik, weder zu bestätigen noch zu dementieren, für Nachrich-

---

[8] D. h. im Rahmen einer Anordnung nach Paragraph 8(4) des RIPA, oben.

[9] Zeugenaussage von Charles Farr, 16. Mai 2014, verfügbar unter: https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf.

[10] "Home Secretary's Defence and Security Lecture", 24. Juni 2014, verfügbar unter: https://www.gov.uk/government/speeches/home-secretarys-defence-and-security-lecture.

[11] "Consultation on the draft Codes of Practice on Interception and Equipment", 6. Februar 2015, verfügbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/401867/Consultation on th e draft Codes of Practice on Interception and Equipmen....pdf.

tensachverhalte beibehalten. Wie oben angedeutet, hatte dies eine wichtige Auswirkung auf die öffentliche Debatte im Vereinigten Königreich. Dr. Arne Hintz konstatiert: „Ein besonderer Aspekt vieler [Medien]Berichte ist eine starke „Vorsichtshaltung" (gelinde gesagt) gegenüber den Fakten (d. h. jene nicht dementierten und nicht dementierbaren Tatsachen, die im Zuge der Snowden-Enthüllungen zum Vorschein kamen) und ein vollständiges Fehlen von Vorsicht gegenüber Behauptungen und Meinungen (insbesondere jenen, die von der Regierung und Spionageagenturen stammen), selbst wenn letztere in direktem Widerspruch zu den bekannten Fakten standen".[12]

„Massenüberwachung" und das Recht auf Privatsphäre

15. Eine Begleiterscheinung der „weder bestätigen noch dementieren"-Politik der Regierung war eine eindeutige und oftmals absurde Ablehnung jeglicher Vorstellung davon, dass das GCHQ Massenüberwachung praktiziert. Im Anschluss an die ersten Snowden-Enthüllungen bestand die britische Innenministerin Theresa May darauf, dass es „kein Programm einer Massenüberwachung und keinen Überwachungsstaat gibt." Sie räumte ein, dass „behauptet wird, das GCHQ nutze ein technisches Schlupfloch in der Gesetzgebung, um externe Kommunikationen – also Kommunikationen, die außerhalb des Vereinigten Königreichs entweder verschickt oder empfangen werden – willkürlich und ohne Genehmigung abzufangen", argumentierte aber, solche Behauptungen seien „Unsinn... externe Kommunikationen wurden im Regulation of Investigatory Powers Act klar und deutlich definiert. Das ist nicht neu und wird auch nicht verborgen."[13] Bei ihrer Aussage vor dem parlamentarischen Intelligence and Security Committee (s. Abs. 44-52) im Oktober 2014 verteidigte May auch die Verschwiegenheitskultur um die Aktivitäten der Nachrichtendienste und die fortgesetzte Regierungspolitik, weder zu bestätigen noch zu dementieren. Der Europäische Gerichtshof für Menschenrechte hat die Anfechtung der Kapazität des Vereinigten Königreichs zur Massenüberwachung und der pauschalen Ausnahme seiner Nachrichtendienste vom britischen Informationsfreiheitsgesetz (s. Absatz 81) zugelassen.

16. Die Regierung argumentiert auch, dass die Massendatenerfassung keine „Verletzung der Privatsphäre" ist, weil: „...wir einen Heuhaufen haben müssen, um die Nadel zu finden, damit wir die Öffentlichkeit schützen können."[14] In ihrer Aussage vor dem Intelligence and Security Committee argumentierte May, dass die Massendatenerfassung keine Massenüberwachung bedeutet, weil „die meisten Daten überhaupt nicht angesehen, nicht berührt werden".[15] Außerdem lehnte sie Bedenken ab, die Speicherung von und der Zugriff auf Kommunikationsdaten seien übermäßig ausgedehnt. Frau May argumentierte, dass Überlegungen zur Privatsphäre erst dann relevant sein sollten, „wenn die Kommunikation geöffnet wird". Außerdem rechtfertigte sie die Massendatenerfassung durch die Regierung damit, dass dies den Aktivitäten kommerzieller Unternehmen entspreche, die massenweise Daten über ihre Kunden sammeln, um gezielte Werbung zu erleichtern. Das Komitee wies darauf hin, dass die Menschen normalerweise ihr Einverständnis zu dieser Art von Datenerfassung geben, auch wenn dies manchmal unwissentlich geschieht. May entgegnete: „Ich glaube, es gibt – zwar keinen schriftlichen Vertrag – aber einen ungeschriebenen Konsens zwischen der Einzelperson und dem Staat, dass der Staat alles in seiner Macht stehende tun wird, um die Einzelperson zu schützen."

17. Im März 2015 rief die Regierung tatsächlich zu einem Ende der Diskussion über die Snowden-Enthüllungen auf. Philip Hammond, Außenminister, meinte, dass die Debatte über die Überwachung „nicht endlos weitergehen darf", und dass es „ganz klar" ist, „dass die Fähigkeit, Massenkommunikationsdaten abzufangen, diese Metadaten einer elektronischen Analyse zu unterziehen und zu versuchen, den winzig kleinen Anteil an Kommunikationen, der von unmittelbaren Sicherheitsinteresse sein kann, zu extrahieren, keine Stärkung der Befugnisse der Nachrichtendienste darstellt. Eher han-

---

[12] s. o. Fußnote 2.

[13] s. o. Fußnote 10.

[14] "Secretive Home Secretary quizzed over UK mass surveillance", Russia Today, 16. Oktober 2014, verfügbar unter: http://rt.com/uk/196468-may-questioned-security-committee/.

[15] "Theresa May: We need to collect communications data 'haystack'", BBC, 16. Oktober 2014, verfügbar unter: http://www.bbc.co.uk/news/uk-politics-29642607.

delt es sich um die Anpassung dieser Befugnisse an die Realitäten des 21. Jahrhunderts".[16] Diese wiederholten Behauptungen stellen eine abgestimmte Strategie des systematischen Leugnens der Dimensionen und Auswirkungen der von Snowden enthüllten internationalen Kommunikationsüberwachung dar.

Durch Snowdens Enthüllungen wurde die „nationale Sicherheit beschädigt"

18. Die Regierung hat mehrfach angegeben, dass die Enthüllungen Snowdens der nationalen Sicherheit des Vereinigten Königreichs geschadet haben – allerdings ohne greifbare Beweise für diese Schäden zu liefern. In den pauschalen Verurteilungen Snowdens und der Journalisten und Medien, mit denen er zusammenarbeitete, ist implizit die Verteidigung der von ihm enthüllten Praktiken enthalten. Außerdem konnte die Regierung, indem sie den Schadensort von einer aufdringlichen Überwachung durch den Staat auf Besorgnisse und Ängste der Öffentlichkeit bezüglich des Terrorismus verlagerte, argumentieren, jetzt seien noch mehr Überwachungsmöglichkeiten erforderlich.

19. Im Oktober 2013 sagte der Premierminister dem Parlament: „Ich finde, Tatsache ist, dass das, was passiert ist, der nationalen Sicherheit geschadet hat, und in vielerlei Hinsicht haben die Vertreter des Guardian selbst zugegeben, dass sie auf höfliche Aufforderung durch meinen nationalen Sicherheitsberater und Kabinettsminister, die in ihrem Besitz befindlichen Dateien zu löschen, dieser Bitte auch Folge geleistet haben. Sie wissen also, dass das, womit sie da zu tun haben, eine Gefahr für die nationale Sicherheit darstellt."[17] Der Guardian meldet eine andere Version der Ereignisse, wobei freundliche Aufforderungen, die Daten entweder zu zerstören oder zu übergeben – angeblich nach dem Motto: „Also gut, Sie hatten Ihren Spaß – jetzt wollen wir die Sachen aber zurück"[18] – zu Androhungen von Strafanzeigen mutierten, sodass man sich beim Guardian entschloss, die Dateien zu löschen, um eine Zensur zu vermeiden.[19] Der damalige Herausgeber der Zeitung, Alan Rusbridger, sagte: „Ich erklärte den britischen Behörden, dass es weitere Kopien in Amerika und Brasilien gebe, sodass sie damit nichts erreichen würden... Aber als es dann offensichtlich war, dass sie uns verklagen würden, zog ich es vor, unsere Kopie zu löschen, anstatt sie ihnen auszuhändigen oder es den Gerichten zu ermöglichen, unsere Berichterstattung einzufrieren."[20]

20. Nach der Intervention durch den Premierminister entschied sich das parlamentarische Home Affairs Select Committee, „Elemente der Beteiligung des Guardian an den Snowden-Enthüllungen und ihrer Veröffentlichung" als Bestandteil der laufenden Untersuchungen im Kampf gegen den Terrorismus zu werten (s. Abs. 48). Im November 2013, bevor diese Verhandlungen im Gang waren, sagte der damalige Leiter des MI6, Sir John Sawers, bei einer separaten Untersuchungsanhörung des Intelligence and Security Committee (s. Abs. 49-52): „Die Enthüllungen Snowdens haben großen Schaden verursacht. Sie haben unsere Operationen in Gefahr gebracht. Es ist klar, dass unsere Gegner sich jetzt vor Freude die Hände reiben. Al-Kaida genießt das Ganze mit Entzückung." Diese Behauptungen wurden vom Leiter des MI5 wiederholt und vom Innenminister und vom Außenminister unterstützt; inzwischen hatte der ehemalige Verteidigungsminister der britischen Staatsanwaltschaft geschrieben und ein Strafverfahren gegen den Guardian verlangt.[21] Bei der Anhörung des Home Affairs Committee im Dezember

---

[16] "Philip Hammond: time to 'move on' from Snowden surveillance revelations," Guardian, 10. März 2015, verfügbar unter: http://www.theguardian.com/world/2015/mar/10/uk-must-move-on-from-surveillance-powers- debate-says-philip-hammond.

[17] "David Cameron criticises the Guardian for publishing Snowden data," BBC, 16 October 2013, available at: http://www.bbc.co.uk/news/uk-politics-24555955.

[18] Simon Jenkins, "So the innocent have nothing to fear? After David Miranda we now know where this leads," Guardian, 20 August 2013, available at: http://www.theguardian.com/commentisfree/2013/aug/20/innocent- fear-david-miranda.

[19] "NSA files: why the Guardian in London destroyed hard drives of leaked files", Guardian, 20. August 2013, verfügbar unter: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.

[20] Alan Rusbridger, "The Snowden Leaks and the Public", The New York Review of Books, 21. November 2013, verfügbar unter: www.nybooks.com/articles/archives/2013/.../snowden-leaks-and-public/.

[21] "Guardian faces fresh criticism over Edward Snowden revelations", Guardian, 10. November 2013, verfügbar unter: http://www.theguardian.com/media/2013/nov/10/guardian-nsa-revelations-edward-snowden.

2013 wurde der Innenminister von Abgeordneten dafür kritisiert, dass er keine Nachweise zur Unterstützung der „melodramatischen Verlautbarungen" und „hochemotionalen Aussagen" der Nachrichtendienste geliefert hatte.[22] Der Premierminister hatte bereits gegenüber Forderungen des Vorsitzenden des Komitees, die Leiter der Nachrichtendienste sollten selbst an den Anhörungen teilnehmen, sein Veto eingelegt.

21. Im April 2014 behauptete Charles Farr, den Ministern sei ein „schlüssiger Nachweis" geliefert worden, dass einzelne Verdächtige und Terrorzellen seit der Veröffentlichung der Informationen über die Überwachungsmöglichkeiten und -methoden vom Radarschirm der Nachrichtendienste verschwunden seien: „Unsere Leistung bei der Terrorismusbekämpfung ist nicht so gut, wie sie sonst hätte sein können".[23] In ähnlicher Weise sagte Theresa May den Abgeordneten im März 2015: „Nach meiner Beurteilung und auch der des Generaldirektors des MI5 haben die Snowden-Enthüllungen schon Schaden angerichtet. Sie haben Auswirkungen auf die Fähigkeit unserer Agenturen gehabt, ihre notwendige Arbeit zu tun. Es wäre gerecht zu sagen, dass dies Folgen nicht nur für die Agenturen im Vereinigten Königreich gehabt hat. Wenn etwas zur Schadensbegrenzung getan wird, so sind dafür Ressourcen erforderlich."[24] Diese Behauptungen wurden von vielen Mainstream-Medien unkritisch akzeptiert. Am 14. Juni 2015 brachte die Sunday Times eine Reihe unbestätigter Behauptungen anonymer Regierungsquellen über die Auswirkungen der Snowden-Enthüllungen in einem Artikel mit der Überschrift „British spies betrayed to Russians and Chinese; Missions aborted to prevent spies being killed" (Britische Spione an Russen und Chinesen verraten; Missionen abgebrochen, um das Töten von Spionen zu verhindern).[25] In dem Artikel wurde behauptet, dass „Russland und China die streng vertrauliche Sammlung von Dateien, die der auf der Flucht befindliche amerikanische Whistleblower Edward Snowden gestohlen hat, geknackt haben, sodass der MI6 in feindlichen Ländern im Einsatz befindliche Agenten zurückziehen musste". Obwohl der Artikel u. a. von Journalisten, die die Snowden-Dokumente kannten, ins Lächerliche gezogen wurde, wurden die Behauptungen von vielen Mainstream-Medien wiederholt.[26]

22. Die nationale Sicherheit wurde auch bemüht, um die neunstündige Festnahme von David Miranda – dem Partner des Journalisten Glenn Greenwald, der die Berichterstattung des Guardian in den USA über die Snowden-Enthüllungen leitete – gemäß Anhang 7 des britischen Terrorismusgesetzes im August 2013 am Flughafen Heathrow zu rechtfertigen. Nach dieser Maßnahme – die ausschließlich Häfen und Transitbereiche von Flughäfen betrifft, bevor die Passagiere durch die Passkontrollen kommen und das eigentliche Großbritannien betreten – können Personen neun Stunden lang ohne ein Recht auf anwaltliche Vertretung festgenommen und ihre Habseligkeiten sieben Tage lang beschlagnahmt werden. Es gibt kein Erfordernis, eine Person wegen einer terrorismusbezogenen Straftat zu verhaften oder anzuklagen – tatsächlich wurde Miranda nie angeklagt, Terrorist zu sein oder zu einer terroristischen Vereinigung zu gehören –, und den Journalisten sowie etwaigem sensiblen Material in ihrem Besitz wird kein Schutz geboten. Miranda hatte verschlüsselte Dateien bei sich, darunter auch 58.000 streng vertrauliche britische Geheimdienstdokumente auf einer externen Festplatte; es wurde alles beschlagnahmt, mit der Begründung, dass eine Veröffentlichung die britische nationale Sicherheit

---

[22] "MPs grill Theresa May over spy chiefs' 'melodramatic soundbites' on NSA files", Guardian, 16. Dezember 2013, verfügbar unter: http://www.theguardian.com/politics/2013/dec/16/theresa-may-mps-spy-chiefs-nsa.

[23] "We have 'conclusive evidence' that Edward Snowden leaks hurt UK national security, say spy chiefs", Daily Mail, 11. April 2014, verfügbar unter: http://www.dailymail.co.uk/news/article-2601977/We-conclusive-evidence- Edward-Snowden-leaks-hurt-UK-national-security-say-spy-chiefs.html.

[24] "'Traitor' Snowden endangered spies with NSA leaks, claim UK security chiefs", Russia Today, 18. März 2015, verfügbar unter: http://rt.com/uk/241869-snowden-may-traitor-cost/.

[25] "British spies betrayed to Russians and Chinese", Sunday Times, 14. Juni 2015, verfügbar unter: https://archive.is/BkuMM#selection-855.0-865.204.

[26] "Snowden files 'read by Russia and China': five questions for UK government", Guardian, 14. Juni 2015, verfügbar unter: http://www.theguardian.com/us-news/2015/jun/14/snowden-files-read-by-russia-and-china-five-questions-for-uk-government.

„ernsthaft schädigen und letztendlich Leben gefährden würde."[27] In einer Klage Mirandas zur Anfechtung der Legalität seiner Inhaftierung vor dem High Court befanden drei Richter im Februar 2014, seine Behandlung sei angesichts der „sehr dringlichen" Interessen der nationalen Sicherheit gerechtfertigt gewesen, auch wenn es sich um „einen indirekten Eingriff in die Pressefreiheit" gehandelt habe. Die Richter weigerten sich zu akzeptieren, dass es sich bei den beschlagnahmten Dateien um „journalistisches Material" handelte, und werteten sie stattdessen als gestohlene Daten, welche die Anwendung von Mechanismen zum Schutz der freien Meinungsäußerung nicht verdienten. Außerdem wiesen die Richter Behauptungen zurück, die Befugnisse nach Anhang 7 seien dazu benutzt worden, das rechtliche Erfordernis einer richterlichen Genehmigung zur Beschlagnahme von Material von Journalisten zu umgehen (s. Abs. 30-31).

III BEGLEITENDE ENTWICKLUNGEN, DIE ZUR ERWEITERUNG DER ÜBERWACHUNGSDEBATTE BEIGETRAGEN HABEN

23. Dieser Abschnitt beschreibt, wie der Umfang der öffentlichen Debatte im Vereinigten Königreich seit den ersten Snowden-Enthüllungen durch Ereignisse, Gerichtsurteile und politische Maßnahmen darüber, wie die Überwachung wahrgenommen oder reguliert wird, erweitert wurde. Dies vermittelt den notwendigen Hintergrund und den Zusammenhang der Debatten zur Überwachungsreform, die in den nachfolgenden Abschnitten erörtert werden.

Vorratsspeicherung von Kommunikationsdaten für den Gesetzesvollzug

24. Nach dem Urteil des Europäischen Gerichtshofs vom April 2014, mit dem die EU-Richtlinie zur Vorratsdatenspeicherung von 2006 aufgehoben wurde, beschleunigte die britische Regierung die inländische Gesetzgebung, um jeder späteren Anfechtungsklage gegen die Vorschriften zur Vorratsdatenspeicherung von 2009 (EG-Richtlinie) zuvorzukommen. Nach diesen Vorschriften waren Kommunikationsdienstleistungsanbieter („KDA" – Internetdienstleistungsanbieter, Mobilfunkbetreiber und Telekommunikationsunternehmen) verpflichtet, Kommunikationsdaten aus E-Mails, Telefongesprächen und Textnachrichten 12 Monate lang zu speichern. Als sekundäre Gesetzgebung nach Maßgabe des die Europäischen Gemeinschaften betreffenden Gesetzes unterlagen die Vorschriften einer gerichtlichen Überprüfung; deswegen brachte die Regierung am 10. Juli 2014 mit der Data Retention and Investigatory Powers Bill ein Notstandsgesetz ein. Durch die Erklärung eines „Notstands" konnte der Gesetzentwurf beschleunigt behandelt und nach weniger als vier Tagen Beratung – von beiden parlamentarischen Häusern – verabschiedet werden.[28]

25. Verwirrend ist in diesem Zusammenhang, dass der Zugriff von Polizei und Nachrichtendiensten auf gemäß dem Data Retention and Investigatory Powers Act (DRIPA) gespeicherte Daten von dem Regulation of Investigatory Powers Act (RIPA) geregelt wird. Anträge zur Ansicht dieser Daten müssen einen Nachweis enthalten, dass der Zugriff sowohl für einen der im RIPA festlegten Zwecke (dies schließt die Staatssicherheit, die Vereitelung und Aufdeckung von Straftaten und die öffentliche Sicherheit ein, ist aber keineswegs darauf beschränkt) „notwendig" als auch im Hinblick auf potenzielle Verletzungen der Privatsphäre einzelner Personen angemessen ist. Sowohl bei der Polizei als auch bei den Nachrichtendiensten werden diese Kriterien intern durch einen „Designated Authorising Officer (eine Person im mittleren Management mit einem Rang, der dem eines „Inspector" oder „Superintendent" in einer Polizeibehörde vergleichbar ist)" bewertet; dabei gibt es keine externe Vorabaufsicht durch die Justizbehörde oder durch ein Überwachungsgericht. Dies hat zu einer sehr hohen Erfolgsquote bei diesen Anträgen geführt; einem Bericht des „Big Brother Watch" (einer Initiative zum Schutz der Privatsphäre) vom Juni 2015 zufolge gewährt sich die Polizei den Zugriff auf Kommunikationsdaten in 96 % aller Fäl-

---

[27] "Miranda documents 'threaten UK security'", Channel 4 News, 30. August 2013, verfügbar unter: http://www.channel4.com/news/miranda-documents-threaten-british-national-security.

[28] "Data Retention and Investigatory Powers Act 2014", Open Right Group, verfügbar unter: https://wiki.openrightsgroup.org/wiki/Data Retention and Investigatory Powers Act 2014.

le. Der Bericht enthüllte auch eine hohe Abweichung bei den Ablehnungsquoten unterschiedlicher Polizeibehörden – von 28 % bis 0,1 % – was erkennen lässt, dass die Leitlinien des RIPA nicht einheitlich durchgesetzt werden.[29] Im Jahr 2014 wurde etwa 460.000 Mal durch Polizei und Strafverfolgungsbehörden und etwa 50.500 Mal durch die Nachrichtendienste auf Kommunikationsdaten zugegriffen.[30] Dennoch behauptete Sir Anthony May, Interception of Communications Commissioner, der für die rückwirkende Aufsicht von Genehmigungsverfahren (s. Abs. 56-58) zuständig ist, dass sein Amt „keine signifikante institutionelle Überbeanspruchung von Kommunikationsdatenbefugnissen durch Polizeikräfte und Strafverfolgungsbehörden festgestellt hat."

26. Der DRIPA ist deswegen kontrovers, weil er in bestimmten Schlüsselbereichen die Überwachungsbefugnisse in den Vorschriften, die er ersetzt hat, effektiv ausweitet. Obwohl die Regierung die Vorschläge lediglich als eine solidere gesetzliche Grundlage für die Vorratsdatenspeicherung vorlegte (Teresa May nannte sie einen „engen und begrenzten" Gesetzentwurf), erweitert das Gesetz die Definition von „Telekommunikationsdienst" auf Dienste wie Webmail und TOR und sieht vor, dass Anträge auf Anordnungen zum Abfangen und auf den Erwerb von Kommunikationsdaten für Unternehmen gestellt werden können, die nicht im Vereinigten Königreich ansässig sind. Der DRIPA ist allgemein in die Kritik von Bürgerbewegungen (Abs. 86-89) und Akademikern (Abs. 96-97) geraten, die gegen die Art und Weise protestieren, wie das Gesetz verabschiedet wurde, und argumentieren, dass es mit dem Urteil des Europäischen Gerichtshofs nicht vereinbar ist. Das Gesetz ist Gegenstand einer laufenden gerichtlichen Überwachung (s. Abs. 73).

27. Die kurze Debatte um den DRIPA ebnete den Weg für künftige Reformen des britischen Überwachungsrechts; dabei setzte die Regierung Bestimmungen ein, die bereits von der US-Regierung im Zuge der Snowden-Enthüllungen genutzt worden waren. Das Gesetz enthält auch eine sog. „Sunset Clause" (Verfallsklausel), nach der es Ende 2016 ausläuft, und sieht eine kürzlich abgeschlossene Überprüfung der Kommunikationsdaten- und Abfangbefugnisse (Review of Communications Data and Interception Powers) vor (s. Abs. 62-68). Eine unabhängiges Aufsichtsgremium für Bürgerrechte (Independent Civil Liberties Oversight Board), offenbar inspiriert durch das Privacy and Civil Liberties Oversight Board, das per Dekret des U.S.-Präsidenten gegründet wurde, wird Aspekte der britischen Überwachungspolitik beaufsichtigen; und ein Sonderbeauftragter für den Austausch von Informationen und Strafverfolgungsdaten wurde ernannt, um die britische Regierung in Verhandlungen mit den KDA, den USA und anderen internationalen Partnern zu vertreten (s. Abs. 59-61).

Die „Schnüffler-Charta"

28. Beim Entwurf des Gesetzes über Kommunikationsdaten, der von Interessengruppen zum Schutz der Privatsphäre „Snoopers' charter" (Schnüffler-Charta) genannt wird, handelte es sich um einen Gesetzentwurf, der von britischen KDA verlangt hätte, dass sie den Bereich der bei ihnen vorhandenen Kommunikationsdaten über ihre Nutzer signifikant erweitern. Zusätzlich zur Vorratsdatenspeicherung, die bereits gemäß dem DRIPA und seiner Vorgängerversion vorhanden war, hätten die KDA u. a. die Internetbesuchshistorie (Weblogs), den Austausch über soziale Medien und Online-Spiele 12 Monate pauschal protokollieren müssen. Die Regierung präsentierte den Gesetzentwurf als notwendig, um es den britischen Sicherheitsbehörden zu ermöglichen, mit dem Wandel in der digitalen Technologie und neuen Online-Kommunikationsdiensten (Skype, Twitter, Facebook, WhatsApp und Snapchat etc.) „Schritt zu halten". Die Regierung argumentierte, dass Kommunikationsdaten aus diesen Quellen für den Zweck der Ermittlung wegen Terrorismus und Schwerverbrechen erfasst und gespeichert werden müssten.

"Police Access to Communications Data", Big Brother Watch, Mai 2015, verfügbar unter: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police- Communications-Data1.pdf.

[30] "Interception of Communications Commissioner's Report 2014", 12. März 2015, verfügbar unter: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf.

29. Das Argument zugunsten einer erweiterten Vorratsdatenspeicherung wurde erstmals im Jahr 2008 im Rahmen des „Interception Modernisation Programme" der damaligen Labour-Regierung vorgebracht. Das Programm wurde im Vorfeld der allgemeinen Wahlen von 2010 auf Eis gelegt, aber unter der neuen Regierungskoalition aus Konservativen und liberalen Demokraten schnell unter einem anderen Namen wiederbelebt, und zwar als „Communications Capabilities Development Programme" (Entwicklungsprogram für Kommunikationsmöglichkeiten). Der Entwurf des Kommunikationsdatengesetzes wurde ordnungsgemäß im Mai 2012 angekündigt,[31] aber unter dem Druck ihrer Anhänger und von Abgeordneten zogen die Liberalen Demokraten ihre Unterstützung für den Gesetzentwurf im darauffolgenden Jahr zurück, verfügbar unter: [Anmerkung des Übersetzers: Die Quellenangabe fehlt an dieser Stelle im Dokument]. Nach dem Wahlsieg der Konservativen Partei im Mai 2015 signalisierte Innenministerin Theresa May ihre Absicht, den Gesetzentwurf wieder einzubringen. Pläne für eine neue Investigatory Powers Bill wurden ordnungsgemäß in der Rede der Königin im Mai 2015 erwähnt, in welcher das legislative Programm der neuen Regierung erklärt wird.

Überwachung und Schutz der Informationsquellen von Journalisten

30. Die Snowden-Enthüllungen haben Journalisten dazu veranlasst, ihre Fähigkeit zum Schutz der Vertraulichkeit ihrer Quellen, einschließlich potenzieller Whistleblower, vor überbreiten Überwachungsbefugnissen der Regierung in Frage zu stellen. Während eine ausdrückliche Genehmigung von einem Richter erforderlich ist, bevor Polizisten Dokumente von einem Journalisten beschlagnahmen können, gilt nach den obengenannten Bestimmungen des RIPA, dass Polizeibeamte in leitenden Positionen dafür zuständig sind, Anträge von Polizisten auf Zugang zu den Telefon- und E-Mail-Daten von Journalisten zu genehmigen.

31. Im Februar 2015 berichtete Sir Anthony May, der Interception of Communications Commissioner (s. Abs. 56-58), dass über einen Zeitraum von drei Jahren 19 Polizeistellen über 600 Anträge zur Ansicht von Telefondaten von Journalisten gestellt hatten, um ihre Quellen auf diese Weise identifizieren zu können. Trotz massiver Kritik führte die Regierung Notstandsleitlinien über den Schutz von Journalistenkommunikationen ein (s. Abs. 83).

Überwachung und anwaltliches Berufsgeheimnis (Aussageverweigerungsrecht)

32. Wie Journalisten, äußern auch Rechtsanwälte angesichts der Massenüberwachung Bedenken wegen des Schutzes vertraulicher Kommunikationen zwischen ihnen und ihren Mandanten. Diese Bedenken würden letztendlich dem IPT vorgetragen werden, nachdem die Snowden-Enthüllungen bei Anwälten, die zwei Männer in ihrer Klage gegen die britische Regierung wegen der Rolle, die sie bei ihrem Transport von China nach Libyen gespielt hatte, vertraten, die Alarmglocken schrillen ließen, dass die staatliche Überwachung eventuell das Recht ihrer Mandanten auf einen fairen Prozess kompromittiert haben könnte. Im Jahr 2004 wurden AbdulHakim Belhaj und Sami al Saadi, beide libysche Staatsbürger und bekannte Gaddafi-Gegner, in China zusammen mit ihren Familien entführt und nach Libyen verfrachtet, wo sie sechs Jahre lang inhaftiert und wiederholten Folterungen ausgesetzt wurden. Dokumente, die nach dem Sturz des Gaddafi-Regimes veröffentlicht wurden, enthüllten die zentrale Rolle der britischen Regierung bei der Auslieferung der zwei Männer.

33. Im Oktober 2014, im Anschluss an die Snowden-Enthüllungen, reichten die Menschrechtsorganisationen Reprieve und Amnesty International eine Klage beim Investigatory Powers Tribunal ein und beschuldigten die Sicherheitsdienste, den Austausch ihrer privaten Mitteilungen sowohl mit Al-Saadi als auch mit Abdul-Hakim abgefangen zu haben. Die Regierung gab zu, dass für die Nachrichtendienste Richtlinien zum Abfangen privater Gespräche zwischen Anwälten und ihren Mandanten gelten, erklär-

[31] Draft Communications Data Bill 2012, Juni 2012, verfügbar unter: http://www.parliament.uk/draft- communications-bill/.

te jedoch, sie werde keine weiteren Einzelheiten angeben, weil dies „dem öffentlichen Interesse schaden oder der nationalen Sicherheit abträglich sein könnte."[32]

34. Im Februar 2015 gestand die Regierung ein, dass wegen des Mangels an klar definierten rechtlichen Schutzmechanismen das Abhören von Unterhaltungen zwischen Anwälten und ihren Mandanten durch die britischen Nachrichtendienste unrechtmäßig gewesen sei. Die britische Regierung hat nunmehr einen aktualisierten Entwurf des Praxiskodex veröffentlicht, um diesen Erfordernissen zu genügen und dafür Sorge zu tragen, dass Abfangschaltungen auf rechtmäßiger Grundlage weiter eingesetzt werden dürfen (s. Abs. 83).

35. Im April 2015 wies das Investigatory Powers Tribunal die britische nationale Sicherheitsüberwachungsagentur GCHQ an, die unter dem anwaltlichen Berufsgeheimnis stehenden Kommunikationen, die sie unrechtmäßig bei Al-Saadi erfasst hatte, zu löschen. Dies war das erste Mal überhaupt, dass das IPT die Nachrichtendienste anwies, unrechtmäßig beschafftes Überwachungsmaterial zu löschen.[33]

Überwachung von Aktivisten und Nichtregierungsorganisationen

36. Nach Enthüllungen über die Infiltration von Protestgruppen durch verdeckte Ermittler der Polizei wurde der RIPA geändert, um „den Umfang einer unabhängigen Aufsicht und Beurteilung von verdeckten Ermittlungen zu vergrößern".[34] Viele der Beamten, die an diesem „Spycops"-Skandal beteiligt waren, wurden nachweislich als Lockspitzel eingesetzt, und manche hatten langzeitige sexuelle Verhältnisse mit Mitgliedern der von ihnen auszuspionierenden Gruppen; in mindestens zwei Fällen zeugten sie auch Kinder. Das Office of Surveillance Commissioners – das für die Aufsicht des Einsatzes verdeckter Überwachung durch Behörden zuständig ist – muss nunmehr am Anfang einer Aktion in Kenntnis gesetzt werden und alle verdeckten Einsätze mit einer Dauer von mehr als 12 Monaten vorab genehmigen. Innerhalb der Polizeibehörden müssen alle Einsätze von verdeckten Ermittlern durch einen Assistant Chief Constable genehmigt werden; alle Einsätze von mehr als 12 Monaten Dauer sind von einem Chief Constable (Polizeipräsident einer Stadt oder Graftschaft) zu genehmigen.

37. Im Juni 2015 bestätigte das Investigatory Powers Tribunal, dass das GCHQ mindestens zwei internationale NRO überwacht hatte: die ägyptische Initiative für persönliche Rechte und das Legal Resources Centre Südafrikas. Das Tribunal weigerte sich offenzulegen, warum die entsprechenden Zielgruppen beobachtet wurden, und – was viel bedeutsamer ist – erachtete die Überwachung nicht als unrechtmäßig, womit es das Recht der britischen Nachrichtendienste, Menschenrechtsorganisationen weltweit zu beobachten, de facto akzeptierte (s. Abs. 84).

Überwachung und außergerichtliche Hinrichtungen

38. Die von Snowden veröffentlichten Dokumente haben die Frage nach der Rolle der britischen Nachrichtendienste bei der Ermöglichung verdeckter US-amerikanischer Drohnenangriffe außerhalb anerkannter Kriegsgebiete entstehen lassen. Eine „streng geheime" Aufzeichnung des GCHQ enthüllte, wie ein gemeinsames Programm der USA, des Vereinigten Königreichs und Australiens mit dem Decknamen „Overhead" einem Drohnenangriff im Jemen im Jahr 2012 Unterstützung lieferte. Rechtsanwältin Jemima Stratford QC (Queen's Counsel), die den aus Vertretern aller Parteien bestehenden parlamentarischen Ausschuss über Drohnen im Jahr 2014 beriet und argumentierte, dass die Vereinbarungen

---

[32] "Abdul-Hakim Belhaj and Fatima Boudcha", Reprieve, verfügbar unter: http://www.reprieve.org.uk/case-study/abdul-hakim-belhaj/.

"'"Secretive court orders GCHQ to destroy stolen documents", Reprieve, 29. April 2015, verfügbar unter: http://www.reprieve.org.uk/press/secretive-court-orders-gchq-to-destroy-stolen-documents/.

[34] "Legislation strengthens independent oversight of undercover police operations", 31. Oktober 2013, verfügbar unter: https://www.gov.uk/government/news/legislation-strengthens-independent-oversight-of- undercover-police-operations.

zur Erfassung und zum Austausch von Nachrichtenmaterial illegal seien,[35] sagte Folgendes zu den „Overhead-Dokumenten": „Wenn das GCHQ Daten an die NSA übertragen hat und dabei wusste, dass diese für die Zielführung von Drohnenangriffen verwendet würden oder werden könnten, dann ist diese Übertragung nach unserer Ansicht wahrscheinlich illegal."[36] Sie fügte hinzu: „Diese Dokumente unterstreichen, warum eine höhere Transparenz im Hinblick auf die offizielle britische Politik dazu beitragen würde, die Rechtmäßigkeit aus inländischer und internationaler Rechtsperspektive zu gewährleisten."

39. Die Regierung bleibt im Hinblick auf gezielte Tötungen bei ihrer strikten Politik, Informationen „weder zu bestätigen noch zu dementieren", eine Haltung, die von dem konservativen Abgeordneten David Davis abgelehnt wird. Er sagte: „Es ist nicht gut, dass sich die Regierung immer hinter ihrem Standardspruch versteckt, zu Sicherheitsfragen keinen Kommentar abzugeben. Der Begriff „außergerichtliche Hinrichtung" ist ein Euphemismus. Wovon wir hier sprechen, ist in Wahrheit Mord... Es ist wichtig, dass die Regierung klar und deutlich sagt, welche Grenzen sie bei der Nutzung ihrer Informationen setzt, und nach welchen Gesetzen und mit wessen Genehmigung diese Informationen ausgetauscht werden." Ein ehemaliger Leiter des GCHQ, David Omand, pflichtete Davis bei und unterzeichnete ein Schreiben mit dem Aufruf an die Regierung, ihre Leitlinien über den Austausch von Nachrichten zum Zweck von verdeckten Drohnenangriffen offenzulegen.

Untersuchungen im Rahmen der Terrorismusbekämpfung und Zugang zu Kommunikationsdaten

40. Bei einer vom Intelligence and Security Committee unternommenen Untersuchung über den von zwei Männern, Michael Adebolajo und Michael Adebowale, verübten Mord an dem britischen Soldaten Lee Rigby in Woolwich im südöstlichen London im Mai 2013 wurde heftige Kritik an den Operationspraktiken ausländischer Kommunikationsdienstanbieter geäußert. Der Ausschuss meinte, wenn die britischen Nachrichtendienste in der Lage gewesen wären, vor dem Mord an Rigby einen Online-Austausch zwischen Adebowale und ausländischen Extremisten zu beobachten, hätte der Angriff *eventuell* verhindert werden können. Aber das Unternehmen, in dessen System der Austausch stattfand (nach den meisten Meldungen Facebook), „sieht sich nicht als dazu verpflichtet an, sicherzustellen, dass es derartige Drohungen identifiziert oder den Behörden meldet. Wir finden das inakzeptabel: Gleichgültig, wie unabsichtlich dies auch gewesen sein mag, gewährt das Unternehmen damit Terroristen einen Unterschlupf".[37] Der Ausschuss stellte fest, dass keiner der wichtigen und großen KDA in den USA proaktiv Inhalte von Nutzern überwacht, und dass sie sich auch nicht verpflichtet fühlen, auf britische Anordnungen nach dem RIPA hin Datenzugriff zu gewähren. „Scheinbar übernehmen sie keinerlei Verantwortung für die von ihnen zur Verfügung gestellten Dienste. Das ist ein sehr ernstes Problem: Die Fähigkeit der Nachrichtendienste, auf Kommunikationen ihrer Zielpersonen zuzugreifen, ist für sie unbedingt notwendig, damit sie terroristische Bedrohungen im Vereinigten Königreich entdecken und verhindern können."

41. Nach den Snowden-Enthüllungen haben sich immer mehr internationale Kommunikationsdienstanbieter dafür entschieden, zum Schutz der Privatsphäre ihrer Kunden Sicherheits- und Verschlüsselungsprotokolle einzuführen bzw. zu verbessern. Als Antwort darauf signalisierte die Regierung, dass sie die Gesetzgebung entsprechend anpassen werde, um zu verhindern, dass Kommunikationen für die Sicherheitsdienste unzugänglich gemacht werden. Obwohl die Wirksamkeit und entsprechende Sicherheit der unterschiedlichen Verschlüsselungsformen noch diskutiert wird, behaupten immer mehr bekannte KDA, dass sie durch die von ihnen eingeführten Maßnahmen nicht mehr in der Lage

---

[35] "Huge swath of GCHQ mass surveillance is illegal, says top lawyer", Guardian, 28. Januar 2014, verfügbar unter: http://www.theguardian.com/uk-news/2014/jan/28/gchq-mass-surveillance-spying-law-lawyer.

[36] "GCHQ documents raise fresh questions over UK complicity in US drone strikes", Guardian, 24. Juni 2014, verfügbar unter: http://www.theguardian.com/uk-news/2015/jun/24/gchq-documents-raise-fresh-questions-over-uk-complicity-in-us-drone-strikes.

[37] ISC-Pressemitteilung, November 2014, verfügbar unter: http://isc.independent.gov.uk/files/20141125 ISC Press Release Woolwich.pdf.

sind, Kommunikationen ihrer Kunden zu entschlüsseln; das bedeutet, selbst wenn sie bereit wären, den Nachrichtendiensten Zugriff auf die entsprechenden Inhalte zu gewähren, könnten sie dies nunmehr nicht mehr tun.

42. Im Januar 2015 hielt Premierminister David Cameron eine Rede, in der er darauf hinwies, dass die Sicherheitsdienste stets in der Lage sein müssen, die Kommunikationen der Menschen zu lesen; er sagte, die Regierung werde „Gesetze einführen, die sicherstellen, dass wir den Terroristen keinen Freiraum gewähren, sicher miteinander zu kommunizieren." Auch wenn er sich nicht dazu äußerte, wie dies in der Praxis erreicht werden könnte, ist der einzig denkbare Weg, dieses Ergebnis zu erzielen, eine Forderung nach „Hintertüren" für die Sicherheitsdienste, oder aber ein Versuch, die Nutzung bestimmter Verschlüsselungsformen und die Anwendungen und Dienste, die davon Gebrauch machen, zu verbieten.

IV. UNTERSUCHUNGEN UND PRÜFUNGEN DURCH DAS BRITISCHE PARLAMENT UND ANDERE WICHTIGE AKTEURE

43. Dieser Abschnitt beschreibt die Einrichtung und, wenn möglich, die Ergebnisse von Überprüfungen unterschiedlicher Elemente der Überwachungspolitik und -praxis, die im britischen Parlament stattgefunden haben, von der britischen Regierung in Auftrag gegeben wurden oder aufgrund gesetzlicher Erfordernisse durchgeführt wurden. Während diese Berichte zunehmend eine Reform der britischen Überwachungsgesetze verlangen, halten sie ausnahmslos eher eine ungenügende Aufsicht als eine exzessive Überwachung für das Kernproblem.

Parlamentarische Ausschüsse

44. Das Intelligence and Security Committee (ISC) ist ein gesetzlicher parlamentarischer Ausschuss, der im Jahr 1994 zur Beaufsichtigung von Ausgaben, Verwaltung und Politik der britischen Nachrichtendienste gebildet wurde. Sein Mandat wurde im Jahr 2013 (vor den Snowden-Enthüllungen) erweitert und umfasst nunmehr ihre operativen Aktivitäten, das militärische Nachrichtenwesen, die Sicherheits- und Geheimdienstaktivitäten der Regierung und die Terrorismusbekämpfung im Innenministerium. Seine neun Mitglieder – die vom Parlament nach Nominierung durch den Premierminister bestellt werden – unterliegen dem Official Secrets Act von 1989 und haben Zugang zu höchstvertraulichem Material. Der Ausschuss führt eine Beweisaufnahme bei Ministern und führenden Beamten der Nachrichtendienste durch, die fast ausschließlich geheim erfolgt. Seine Glaubwürdigkeit, Unparteilichkeit und Wirksamkeit werden schon lange in Frage gestellt. Der Direktor der Menschenrechts-NRO Liberty, Shami Chakrabarti, kommentierte: „Das ISC hat sich selbst wiederholt als einfaches Sprachrohr für die Spione entpuppt – so ahnungslos und ineffektiv, dass es nur Edward Snowden zu verdanken ist, dass es eine minimale Ahnung von den Possen der Nachrichtendienste hatte."[38]

45. Am 7. Juni 2013, nach den ersten Snowden-Enthüllungen darüber, dass das GCHQ über das Prism-Programm Daten erhalten hatte, gab das ISC bekannt, dass es „sehr bald einen vollständigen Bericht vom GCHQ erhalten und entscheiden wird, welche weiteren Maßnahmen zu ergreifen sind, sobald diese Informationen vorliegen."[39] Am 17. Juli 2013 gab der Ausschuss bekannt, dass er detaillierte Beweise vom GCHQ analysiert hat und zu dem Schluss gekommen ist, dass mit der Nutzung von Prism durch die Organisation für den Zugang zu den Inhalten privater Kommunikationen „britisches Recht weder umgangen wurde noch versucht wurde, es zu umgehen".[40] Das ISC stellte fest, dass im-

[38] "Intelligence report branded 'clueless' by Liberty director", ITV News, 12. März 2015, verfügbar unter: http://www.itv.com/news/update/2015-03-12/intelligence-report-branded-clueless-by-libertv-director/.

[39] ISC-Pressemitteilung, 7. Juni 2013, verfügbar unter: http://isc.independent.gov.uk/news-archive/7iune2013.

[40] "Statement by the ISC regarding GCHQ's alleged access to the US PRISM programme", 17. Juli 2013, verfügbar unter: http://isc.independent.gov.uk/files/20130717 ISC statement GCHQ.pdf.

mer, wenn das GCHQ Informationen von den USA erbeten hat, „bereits eine von einem Minister unterzeichnete Anordnung zum Abfangen vorlag". Während dies in rechtlicher Hinsicht streng der Wahrheit entsprach, verhüllt die Implikation, dass diese Überwachung gezielt ist, die Tatsache, dass immense Datenmengen ausgetauscht werden, um die „Gezieltheit" zu ermöglichen.

46. Insgesamt war die „Untersuchung" des ISC extrem begrenzt; es wurden lediglich Fälle untersucht, in denen das GCHQ Daten aus den USA *angefordert* hat. Sie befasste sich nicht mit der Einschätzung der Legalität der Tatsache, dass die NSA den britischen Nachrichtendiensten die persönlichen Daten britischer Staatsbürger und im Vereinigten Königreich lebender Personen lieferte. Die Untersuchung befasste sich auch nicht damit, was passierte, als US-Nachrichtendienste ihren britischen Pendants freiwillig Informationen anboten. Die Untersuchung konzentrierte sich nur auf Fälle, in denen der Inhalt von Kommunikationen abgefangen worden war; dabei ließ sie die immensen von Prism erfassten Datenmengen unberücksichtigt. Das eigene Internet-Überwachungsprogramm des GCHQ, Tempora, wurde nicht einmal erwähnt. Was jedoch bei der Untersuchung festgestellt wurde, war, dass eine Einschätzung des ISC notwendig ist, ob der legislative Rahmen des Vereinigten Königreichs zur Regulierung des Zugangs zu privaten Kommunikationen im digitalen Zeitalter noch seinen Zweck erfüllt.
47. Am 17. Oktober 2013 gab das ISC bekannt, dass die Untersuchung des Ausschusses über die Eignung des britischen legislativen Rahmens wegen allgemeiner Bedenken über den Umfang der Überwachungsmöglichkeiten der britischen Nachrichtendienste erweitert wird, um festzustellen, ob gegenwärtig ein vernünftiges Gleichgewicht hergestellt ist zwischen „unserem individuellen Recht auf Schutz der Privatsphäre und unserem kollektiven Recht auf Sicherheit."[41] Damit die „gesamte Bandbreite an Meinungen zu diesen Fragen" berücksichtigt werden konnte, erging im Zuge der Untersuchung die Einladung zur Abgabe schriftlicher Nachweise, auch von der Öffentlichkeit, zusätzlich zu den geheimen Anhörungen in Bezug auf streng vertrauliche Beweisaufnahmen.

48. Im Mai 2014 veröffentlichte das Home Affairs Select Committee einen Bericht über die britischen Möglichkeiten zur Terrorismusbekämpfung. Nach den Snowden-Enthüllungen hatte der Ausschuss eine Anhörung anberaumt, die sich speziell mit ihren Implikationen für die nationale Sicherheit befasste (s. Abs. 20 oben). Der Abgeordnete Keith Vaz nannte die Enthüllungen eine „peinliche Anklage" des britischen Systems demokratischer Kontrollen.[42] In dem Bericht wurde eine Reform der Aufsicht von MI5, MI6 und GCHQ gefordert und festgestellt, dass der „Spielraum, der den Kongressausschüssen [in den USA] zur Prüfung nachrichtendienstlicher Angelegenheiten durch die Exekutive gewährt wird, vielleicht der wichtigste Unterschied zwischen dem US-System und dem System des Vereinigten Königreichs ist, wo sich die Regierung konsequent weigert, anderen Ausschüssen als dem ISC Fragen über die Arbeit der Sicherheits- und Nachrichtendienste zu erlauben. Angesichts der Tatsache, dass einige wichtige Fragen im Rahmen der Arbeit der Justizausschüsse aufgeworfen und debattiert wurden, ist es vielleicht aufschlussreich, dass die Debatte in den USA, wo mehr Abgeordnete die Arbeit derartiger Dienste in Augenschein nehmen können, wesentlich hitziger war."[43]

49. Am 12. März 2015 veröffentlichte das ISC nach einer 18-monatigen Untersuchung seinen zweiten Bericht: „Privacy and Security: A modern and transparent legal framework" (Privatsphäre und Sicherheit: Ein moderner und transparenter rechtlicher Rahmen).[44] Seine zwei wichtigsten Feststellungen: (i) „Die britischen Nachrichten- und Sicherheitsdienste versuchen nicht, das Gesetz zu umgehen"; und (ii) „Der rechtliche Rahmen ist unnötig kompliziert und – vor allem – fehlt es ihm an Transparenz". Die „wichtigste Empfehlung", die sich aus der Untersuchung ergab, war, „dass der gegenwärtige rechtliche

---

[41] ISC-Pressemitteilung, 17. Oktober 2013, verfügbar unter: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131017 ISC statement privacy and security inqui ry.pdf.

[42] "MPs: Snowden files are 'embarrassing indictment' of British spying oversight", Guardian, 9. Mai 2014, verfügbar unter: http://www.theguardian.com/uk-news/2014/may/09/edwa rd-snowden-mps-commons-report- spying.

[43] "Home Affairs Committee - Seventeenth Report: Counter-terrorism", 30. April 2014, verfügbar unter: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23103.html.

[44] "Privacy and Security: A modern and transparent legal framework", ISC, 12. März 2015, verfügbar unter: http://isc.independent.gov.uk/files/20150312 ISC P+S+Rpt(web).pdf.

Rahmen durch ein neues Gesetz zur Regelung der Nachrichten- und Sicherheitsdienste ersetzt werden sollte. Darin muss genau festgelegt werden, mit welchen Interventionsbefugnissen die Dienste ausgestattet sind, zu welchen Zwecken sie diese einsetzen können, und welche Genehmigung erforderlich ist, bevor sie dies tun können."

50. In dem Bericht des ISC wurden erstmals die „massenhaften Abfangmöglichkeiten" des GCHQ bestätigt; es wurde aber auch festgestellt, dass die Praxis „mit einer großen Menge an E-Mails verbunden sein kann, was aber" angesichts der im Einsatz befindlichen Zielauswahl- und Filtersysteme „nicht gleichbedeutend ist mit einer pauschalen Überwachung, und auch nicht mit einer wahllosen Überwachung". Das ISC argumentierte, weil das GCHQ nur auf einen kleinen Prozentsatz der globalen Internetstruktur Zugriff habe, könnten seine Praktiken nicht als „pauschale Abhör- bzw. Abfangmaßnahmen" dargestellt werden; dabei wurde aber die Tatsache außer Acht gelassen, dass durch enge Zusammenarbeit mit den Nachrichtendiensten anderer Länder *de facto* ein breiterer Zugang erzielt wird. Diese Feststellungen ernteten heftige Proteste von Menschenrechtsgruppen und Aktivisten für den Schutz der Privatsphäre (s. Abs. 87). Von großer Bedeutung ist, dass der ISC-Bericht keine Empfehlungen darüber enthielt, wie der Datenaustausch mit den USA und anderen Ländern reguliert werden sollte.
51. Im Namen des Ausschusses sagte Hazel Blears, damals Abgeordnete der Labour-Partei: „Wir haben festgestellt, dass die Art und Weise, in der die Dienste ihre Möglichkeiten nutzen, genehmigt, rechtmäßig, notwendig und angemessen ist. Wir stellten aber auch fest, dass es eine gewisse Verwirrung und einen Mangel an Transparenz über die Art und Weise gibt, wie dies in unserem Rechtssystem genehmigt wird." Dieser Mangel an Transparenz, so die Warnung des Berichts, „könnte dahingehend falsch ausgelegt werden, dass den Diensten ein „Blankoscheck" zur Durchführung aller Aktivitäten, die sie für erforderlich halten, ausgestellt wird."[45]

52. Aufschlussreich ist, dass der Bericht den Mangel an gesetzlicher Aufsicht über „bulk personal datasets" (massenhafte personenbezogene Datensätze) bestätigt. Die Regierung antwortete mit einer Stellungnahme, mit der Sir Mark Waller, dem Intelligence Services Commissioner „gesetzliche Aufsichtsbefugnisse" eingeräumt wurden (s. Abs. 57).

Das Royal United Services Institute

53. Nachdem es Nick Clegg, damals stellvertretender Premierminister und Chef der Liberaldemokraten, im März 2014 nicht gelungen war, seine konservativen Koalitionspartner von der Notwendigkeit einer breit angelegten Untersuchung zur Überprüfung der Rechenschaftsstruktur britischer Nachrichtendienste zu überzeugen, beauftragte er das Royal United Services Institute mit einer unabhängigen Überprüfung von Überwachungspraktiken im Internet und ihrer Kontrolle und Beaufsichtigung.

54. Die RUSI-Überprüfung orientiert sich an der von US-Präsident Barack Obama im Januar 2014 über „Big Data" und Privatsphäre in Auftrag gegebenen Überprüfung. Clegg schrieb im Guardian, dass „die Qualität der Debatte in den USA in wenig schmeichelhaftem Kontrast zur gedämpften Diskussion auf dieser Seite des Atlantiks steht".[46] Die wichtigsten Punkte der Überprüfung: (i) Beratung zu Legalität, Wirksamkeit und den Implikationen für die Privatsphäre von britischen Überwachungsprogrammen, insbesondere, wie dies durch die Snowden-Enthüllungen offenbart wurde; (ii) Prüfung potenzieller Reformen gegenwärtiger Überwachungspraktiken, einschließlich zusätzlicher Schutzmechanismen gegen den Missbrauch personenbezogener Daten sowie Alternativen zur Datenerfassung und Vorratsspeicherung von Massendaten; (iii) Einschätzung, wie die Möglichkeiten des Gesetzesvollzugs und im Nachrichtenbereich angesichts des technologischen Wandels aufrechterhalten und dabei auch die

---

[45] Oben

[46] "Edward Snowden's revelations made it clear: security oversight must be fit for the internet age", Guardian, 3. März 2014, verfügbar unter: http://www.theguardian.com/commentisfree/2014/mar/03/nick-clegg-snowden- security-oversight-internet-age.

Grundsätze der Ausgewogenheit, Notwendigkeit und des Schutzes der Privatsphäre respektiert werden können.[47]

55. Das RUSI ist eine eingetragene karitative Organisation, deren Geschichte bis ins Jahr 1829 zurückgeht. Obwohl sie regierungsunabhängig ist, ist sie nach David Wearing von der University of London eigentlich mehr als „Gebilde des britischen Staates und des militärischen Establishments zu sehen, ohne die sie weder gegründet worden wäre noch heute in erkennbarer Form bestehen würde".[48] Die zwölf Mitglieder des Independent Surveillance Review Panel des RUSI sind ehemalige Leiter des GCHQ, MI5, MI6 und des Nachrichtendirektoriums der Metropolitan Police, Professoren aus den Bereichen Journalismus, Rechtswissenschaften, Informatik, Geschichte und Philosophie, der Gründer des Online-Reisebüros Lastminute.com und ein ehemaliger Leiter von Nominet, der britischen Domain-Registratur.[49] Nach der Beschreibung des RUSI sind in diesem Gremium "alle wichtigen Interessen im Überwachungsbereich, die Industrie, die Regierungspolitik, die Sicherheit, die geisteswissenschaftliche Forschung, die Bürgerrechtsinteressen und die parlamentarischen Belange" vertreten. Es fanden keine öffentlichen Verfahren oder Aufforderungen zu Beweisaufnahmen und auch kein offenbarer Kontakt zu Bürgerrechtsorganisationen oder Menschenrechtsgruppen statt. Der Bericht des Gremiums soll Mitte Juli 2015 erscheinen.

Interception of Communications Commissioner

56. Sir Anthony May, Interception of Communications Commissioner (ICC), ist verantwortlich für die Überprüfung, wie Nachrichtendienste, Polizeikräfte und Behörden den RIPA verwenden, um Kommunikationen abzufangen und Kommunikationsdaten zu erfassen und offenzulegen. Der ICC ist dafür verantwortlich, dass diese Gremien im Rahmen ihrer rechtlichen Verantwortlichkeiten nach dem Gesetz handeln, und überprüft die Rolle des Innenministers bei der Ausstellung von Abfanganordnungen. Die Ausübung dieser Funktionen wird in einem zweimal jährlich erscheinenden Bericht dokumentiert (bis zur Verabschiedung des DRIPA wurden die Berichte jährlich erstellt). Bei seiner Aussage vor dem House of Commons Home Affairs Committee beschrieb May den RIPA als „ein extrem schwer zu verstehendes Gesetz".[50]

57. Der ICC ist einer von drei nach dem RIPA ernannten Kommissaren zur Gewährleistung einer unabhängigen Aufsicht und Kontrolle von Überwachungsfunktionen. Die Beaufsichtigung der Nachrichtendienste (außer Abfangpraktiken) erfolgt durch Sir Mark Waller, den Intelligence Services Commissioner. Und für die Aufsicht der verdeckten Überwachung an öffentlichen und privaten Plätzen, den Einsatz von verdeckten Ermittlern für Nachrichtenquellen und Eingriffe in Eigentumsrechte ist Chief Surveillance Commissioner Sir Christopher Rose zuständig. Jeder Kommissar ist ein vom Premierminister ernannter pensionierter Richter des High Court oder Appeal Court und ist ihm gegenüber berichtspflichtig. Außerdem überprüft der Surveillance Camera Commissioner Tony Porter den Einsatz von verdeckten Videoüberwachungssystemen (sog. „CCTV") nach Maßgabe eines Verhaltenskodex. Sowohl Berichte des ISC als auch des Independent Reviewer of Terrorism Legislation der Regierung enthalten Empfehlungen zur Reform des Kommissarsystems; ersteres sprach sich für Personal- und Ressourcenaufstockungen sowie für eine größere Rolle jedes Kommissars aus, und letzterer forderte die Zusammenlegung der drei Stellen unter einem neuen Gremium, der Independent Surveillance and Intelligence Commission (s. Abs. 65).

---

[47] "Independent Surveillance Review Panel Announced", RUSI News, 12. Juni 2014, verfügbar unter: https://www.rusi.org/news/ref:N5399836649AAC/#.VZPI1EaHAeW.

[48] "Why is the BBC presenting RUSI as objective analysts of the Middle East?", Open Democracy, 12. Juni 2015, verfügbar unter: https://www.opendemocracy.net/ourbeeb/david-wearing/why-is-bbc-presenting-rusi-as-objective-analysts-of-middle-east.

[49] s. o. Fußnote 47.

[50] "Law on GCHQ is complex, says watchdog", Guardian, 11. Februar 2014 , verfügbar unter: http://www.theguardian.com/uk-news/2014/feb/11/gchq-number-personal-data-intercepts-law-too-many-official.

58. In seinem Jahresbericht für 2013, der im April 2014 veröffentlicht wurde, sprach der ICC direkt Bedenken an, dass Überwachungsbefugnisse missbraucht würden, und verteidigte die Überwachungspolitik und Praktiken innerhalb seines Bereichs energisch; in dem Bericht heißt es: „Die Behörden missbrauchen ihre Befugnisse nach RIPA Teil I nicht, um ein wahlloses massenhaftes Eindringen in die Privatsphäre gesetzestreuer britischer Bürgerinnen und Bürger zu betreiben. Es wäre gänzlich illegal, wenn sie dies täten". Außerdem sagte May, dass ihm „ganz klar ist, dass jedes Mitglied der Öffentlichkeit, das sich nicht mit potenziellen Terroristen, Schwerverbrechern oder Individuen verbindet, die potenziell an Aktionen beteiligt sind, die zu nationalen Sicherheitsproblemen für das Vereinigte Königreich führen könnten, sich darauf verlassen kann, dass keiner der Abfangdienste, die unter meiner Aufsicht stehen, auch nur das geringste Interesse daran hat, seine E-Mails, seine telefonischen oder brieflichen Kommunikationen oder seine Nutzung des Internets zu überprüfen, und sie tun dies nicht in einem Umfang, der berechtigterweise als signifikant bezeichnet werden könnte." May sagte auch, dass die „britischen Nachrichtendienste die inländischen Aufsichtssysteme nicht umgehen, indem sie Material über britische Staatsbürger von US-Diensten beziehen, das nicht rechtmäßig durch Abfangen im Vereinigten Königreich erlangt werden könnte".[51] Es ist jedoch wichtig hervorzuheben, dass das Mandat des ICC auf jene Aktivitäten beschränkt ist, die in den Anwendungsbereich des RIPA fallen, wobei viele Kommunikationsdatenerfassungsaktionen außerhalb seines Zuständigkeitsbereichs stattfinden. Wie der Kommissar selbst bestätigte, „bin ich nicht zur Aufsicht aller Aktivitäten der Nachrichtendienste ernannt oder befugt, sondern nur für diejenigen, die in Paragraph 57(2) des RIPA aufgeführt sind.[52] Trotz der scheinbar vehementen Verteidigung der von Snowden enthüllten Überwachungsarten wird daher in Mays Bericht nichts über Programme wie Tempora oder Prism oder aber die Verbindungen zwischen den Nachrichtendiensten und den Kommunikationsdienstanbietern erwähnt. Seine Behauptung, dass die Nachrichtendienste keinerlei Interesse an den Kommunikationen von „normalen" Mitgliedern der britischen Öffentlichkeit, geschweige denn an denen normaler Bürger anderswo haben, ist deshalb meiner Meinung nach fraglich.

Sonderbeauftragter für den Austausch von Informationen und Strafverfolgungsdaten

59. Sir Nigel Scheinwald, ein ehemaliger britischer Botschafter in Washington, arbeitet seit September 2014 als Sonderbeauftragter des Premierministers für den Austausch von Informationen und Strafverfolgungsdaten.[53] Er wurde gebeten, über Alternativen zur pflichtmäßigen Speicherung von Telekommunikationsdaten nach dem Data Retention Investigatory Powers Act (s. oben, Abs. 24-27) und nach der sogenannten „Schnüffler-Charta (s. oben, Abs. 28-29) zu berichten.

60. Der Bericht Scheinwalds wurde im Frühjahr 2015 fertig gestellt, aber vom Cabinet Office als „streng geheim" deklariert und der Öffentlichkeit vorenthalten. Die Regierung behauptet, dass es kein Erfordernis gibt, den Bericht zu veröffentlichen, weil der Sonderbeauftragte „keine öffentliche Überprüfung durchführt." Die Schlussfolgerungen wurden an die Zeitung The Guardian weitergegeben, und nach Beschwerden von Interessengruppen für den Schutz der Privatsphäre, die Regierung versuche, die Debatte über die Überwachungsreform zu unterdrücken,[54] wurde eine zweiseitige Zusammenfassung veröffentlicht.[55]

---

[51] "2013 Annual Report of the Interception of Communications Commissioner", April 2014, verfügbar unter: http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

[52] "Sir Anthony May's response to the Article published in the Independent", ICC Office, 13. März 14, verfügbar unter: http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top.

[53] "Sir Nigel Sheinwald appointed Special Envoy on intelligence and law enforcement data sharing", Cabinet Office, 19. September 2014, verfügbar unter: https://www.gov.uk/government/news/sir-nigel-sheinwald- appointed-special-envoy-on-intelligence-and-law-enforcement-data-sharing.

[54] "Secret report urges treaty forcing US web firms' cooperation in data sharing". Guardian, 2. Juni 2015, verfügbar unter: http://www.theguardian.com/world/2015/iun/02/web-firms-data-sharing-secret-treatv.

[55] "Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing - Sir Nigel Sheinwald", verfügbar unter:

61. Die Zusammenfassung enthält Hinweise auf die Wichtigkeit eines „begrenzten und angemessenen Zugriffs auf private Mitteilungen" und auf die Auswirkungen von Verschlüsselung und rechtlichen Reformen auf die „Möglichkeiten der Nachrichten- und Gesetzesvollzugsdienste, auf Daten in lesbarer Form zuzugreifen". Die Zusammenfassung enthält vier „längerfristige Vorschläge": (i) Verbesserung der „Zusammenarbeit zwischen Regierungen" und des „Datenaustauschs zwischen gleichgesinnten Ländern"; (ii) Reform des Amtshilfeabkommens US-UK Mutual Legal Assistance Treaty, um eine schnellere und reagiblere Bearbeitung von Datenanforderungen zu ermöglichen; (iii) Entwicklung eines neuen internationalen Rahmens, der es den britischen Diensten ermöglichen wird, „den Zugang zu Inhalten von Fällen im Bereich Schwerverbrechen und Terrorismusbekämpfung durch direkte Anfragen an [U.S.-KDA] zu erlangen"; (iv) durch die Verbesserung der Transparenz im Hinblick auf die Anzahl und Art unserer Anforderungen an aus- und inländische Kommunikationsdienstanbieter wird die Bearbeitung schneller und einfacher. Scheinwalds Vorschläge stellen eine glaubwürdige Alternative zur Erlangung der erklärten Ziele der „Schnüffler-Charta" dar, die – als sie zuletzt in Form des Gesetzentwurfs für Kommunikationsdaten im Jahr 2012 vorgelegt wurde – Bestimmungen enthielt, die britische Kommunikationsdienstanbieter dazu zwingen sollten, personenbezogene Daten mit Ursprung aus US-Gesellschaften, die sich weigerten, britischen Anträgen auf Datenzugriff freiwillig Folge zu leisten, in ihren Netzwerken zu erfassen.

Independent Reviewer of Terrorism Legislation

62. Im Juli 2014, nach Maßgabe des Data Retention and Investigatory Powers Act, wurde David Anderson, der Independent Reviewer of Terrorism Legislation, angewiesen, eine breitgefächerte Überprüfung der erforderlichen ermittlerischen Möglichkeiten und Befugnisse der Justizvollzugs- und Nachrichtendienste und des regulatorischen Rahmens, innerhalb dessen diese Möglichkeiten und Befugnisse ausgeübt werden sollten, durchzuführen.

63. Der Independent Reviewer ist mit der Aufsicht der Durchführung britischer Gesetze zur Terrorismusbekämpfung und der Unterrichtung der Öffentlichkeit und der Förderung der politischen Debatte durch regelmäßige Berichte an das Parlament betraut. Die gesetzlichen Funktionen dieser Aufgabe wurden durch den Counter-Terrorism and Security Act 2015 zur Überprüfung neuerer Gesetze zur Terrorismusbekämpfung erweitert, obwohl der Independent Reviewer nicht in der Lage ist, Befugnisse zu überprüfen, die nicht ausdrücklich zum Zweck der Terrorismusbekämpfung ausgelegt sind. Durch dieses Gesetz wurde auch ein Privacy and Civil Liberties Board (PCLB) gegründet, inspiriert durch sein US-Gegenstück, den Privacy and Civil Liberties Oversight Board. Laut Anderson „verrät die Bezeichnung des neuen Gremiums nur wenig über seine tatsächlichen Funktionen"; er fügte hinzu: „In einer gut geordneten Welt wären solche Angelegenheiten das Thema einer Beratung und gut durchdachten Maßnahme im Vorwege der eigentlichen Gesetzgebung gewesen".[56] Der PCLB war ursprünglich gegründet worden, um den Independent Reviewer zu ersetzen, wird nunmehr aber unter der Leitung und Kontrolle Andersons arbeiten.

64. Andersons Bericht mit dem Titel „A Question of Trust" wurde am 11. Juni 2015 veröffentlicht.[57] Mit ihm war beabsichtigt, „die Öffentlichkeit zu informieren und die politische Debatte über diese Angelegenheiten zu fördern, die schlimmstenfalls polarisiert, maßlos und durch technische Missverständnisse geprägt sein kann"; zur „Zufriedenstellung der Mehrheit, die weitgehend das gegenwärtige Ausmaß an ermittlerischen Tätigkeiten und Beaufsichtung akzeptiert"; und „dazu beizutragen, Vertrauen unter

---

https://www.gov.uk/government/uploads/system/uploads/attachment data/file/438326/Special Envoy wor k summary final for CO website.pdf.

[56] "Independent Review and the PCLB", Independent Reviewer of Terrorism Legislation, 31. Januar 2015, verfügbar unter: https://terrorismlegislationreviewer.independent.gov.uk/independent-review-and-the-pclb/.

[57] "A Question of Trust - Report of the Investigatory Powers Review", Independent Reviewer of Terrorism Legislation, 11. Juni 2015, verfügbar unter: https://terrorismlegislationreviewer.independent.gov.uk/wp- content/uploads/2015/06/IPR-Report-Print-Version.pdf.

den Skeptikern sowohl im Vereinigten Königreich als auch im Ausland aufzubauen". Anderson wiederholte die wichtigsten Feststellungen des früheren ISC-Berichts (s. oben, Abs. 49) und zog den Schluss, dass „das derzeitige Recht fragmentiert und undurchsichtig ist, ständig auf dem Prüfstand steht und variabel ist im Hinblick auf den Schutz, den es unschuldigen Personen gewährt... es ist Zeit, einen Schlussstrich zu ziehen". Der Bericht enthält 124 separate Empfehlungen in dieser Hinsicht.

65. Acht der Empfehlungen sind besonders signifikant im Hinblick auf ihre potenziellen Auswirkungen auf die Überwachungsreform. (i) Ein neues Gesetz sollte formuliert werden, das „in seinem Geltungsbereich umfassend und für die Menschen in der ganzen Welt verständlich ist." Es würde als Ersatz für den gegenwärtigen Wildwuchs an verwirrenden Gesetzen dienen; es handele sich hier um einen Zustand, der „undemokratisch, unnötig und – auf lange Sicht – unduldbar ist." (ii) Die DRIPA-Befugnisse, die von britischen KDA verlangen, Kommunikationsdaten für den Justizvollzug und zu Sicherheitszwecken zu speichern (s. oben, Abs. 24-27) sollten weiterhin in Kraft bleiben, aber rechtlichen Einschränkungen unterliegen. (iii) Die Möglichkeiten zur Massendatenerfassung sollten erhalten bleiben, „aber nur nach Maßgabe strenger, zusätzlicher Sicherheitsvorkehrungen" und zusätzlich zu einer neuen und geringeren Befugnis nur zur Erfassung von Massenkommunikationsdaten. (iv) Der Fall "Schnüffler-Charta" (s. oben, Abs. 28-29) ist noch unklar. Gesetze, die KDA dazu zwingen, Web-Protokolle aufzubewahren, sollten erst eingeführt werden, „wenn ein detaillierter Einsatzfall ermittelt wurde und eine rigorose Beurteilung der Legalität, der wahrscheinlichen Wirksamkeit, der Zudringlichkeit und Kosten" dieser Datenvorhaltung erfolgt ist. (v) Die Unterscheidung zwischen ‚internen' und ‚externen' Kommunikationen ist im Umfeld des Internet veraltet und sollte aufgegeben werden. (vi) Eine richterliche Genehmigung (durch Justizkommissare) sollte für alle Abfanganordnungen erforderlich sein; die Rolle der Minister sollte auf den Hinweis beschränkt sein, dass manche Anordnungen im Interesse der nationalen Sicherheit notwendig sind. (vii) Eine richterliche Genehmigung sollte erforderlich sein, wenn die Polizei Kommunikationsdaten von Rechtsanwälten, Journalisten und anderen verlangt, die vertrauliche Informationen erhalten (s. Abs. 82-84). (viii) Die drei vorhandenen Kommissare, die sich mit der Überwachung befassen (s. oben, Abs. 57) sollten durch eine neue Independent Surveillance and Intelligence Commission ersetzt werden; das wäre dann ein "regulatorischenes Gremium mit guter Ressourcenausstattung und mit dem Blick nach außen, bestehend aus Richtern a. D., welches die richterliche Genehmigung aller Anordnungen wahrnehmen, umstrittene und sensible Anträge auf Kommunikationsdaten genehmigen und Orientierungshilfe geben könnte.

66. Anderson erklärte, dass er sich weitgehend von der Legitimität der „Massenüberwachung" im Rahmen von Massen-Abfangaktionen überzeugt hatte, wobei er diese Position relativierte, indem er betonte: „Es ist nicht meine Funktion, eine rechtliche Beurteilung anzubieten, insbesondere in einem Fall, über den von einem höchstrichterlichen Gremium befunden wird" (ein Hinweis auf schwebende Verfahren vor dem Europäischen Gerichtshof für Menschenrechte, s. Abs. 70-72). Er stellte jedoch auch fest, dass Fallstudien des GCHQ „bei mir nicht den geringsten Zweifel darüber hinterlassen, dass Massen-Abfangaktionen, wie sie gegenwärtig zur Anwendung kommen, eine wertvolle Rolle beim Schutz der nationalen Sicherheit spielen. Das bedeutet natürlich nicht unbedingt, dass sie ausgewogen sind; darüber haben die Gerichte zu befinden."

67. Andersons radikalster Vorschlag, und zwar, dass Minister ihre Befugnisse zur Genehmigung von Abfanganordnungen an richterliche Behörden abgeben sollten, wurde bereits vom Premierminister abgelehnt, dessen Sprecherin betonte, dass die Justizvollzugs- und Nachrichtendienste in der Lage sein müssen, „schnell und wirksam auf Bedrohungen der nationalen Sicherheit oder auf Schwerverbrechen zu reagieren".[58]

[58] "UK intelligence agencies should keep mass surveillance powers, report says", Guardian, 11. Juni 2015, verfügbar unter: http://www.theguardian.com/world/2015/jun/11/uk-intelligence-agencies-should-keep-mass- surveillance-powers-report-gchq.

68. Innenministerin Theresa May reagierte auf den Bericht mit einem Versprechen, die gesetzlichen Regelungen zu den Ermittlungsbefugnissen komplett zu überholen. Sie sagte, dass Andersons Bericht – zusammen mit dem ISC-Bericht und der bevorstehenden RUSI-Überprüfung – eine sichere Grundlage für die Gesetzgebung darstelle. May sagte gegenüber dem Parlament, sie werde im Herbst 2015 einen Entwurf eines Überwachungsgesetzes veröffentlichen und gehe davon aus, dass das neue Gesetz noch im Jahr 2016 verabschiedet wird.

V RICHTERLICHE ÜBERPRÜFUNG UND ÜBERWACHUNGSREFORM

69. Dieser Abschnitt vermittelt eine Übersicht der richterlichen Überprüfung von Überwachungsbefugnissen, die von Nichtregierungsorganisationen und anderen kritischen Interessengruppen, die sich mit fundamentalen Rechten und demokratischen Kontrollen befassen, angestrebt wird. Dabei vermittelt er gleichzeitig eine Übersicht der materiellrechtlichen Positionen dieser Organisationen im Hinblick auf die Ausübung und demokratische Kontrolle von Überwachungsaktivitäten. In einem Klima mäßiger Debatten über die Überwachung haben diese Fälle dafür gesorgt, dass das Thema in der Öffentlichkeit bleibt, und einen laufenden Gegenpol zu den Darstellungen und Verschleierungstaktiken der Regierung gebildet. Dieser Abschnitt enthält auch eine Zusammenfassung legislativer und nichtlegislativer Reformen von Überwachungsrecht und -praktiken, die sich aus den Klagen der NRO ergeben haben.

Massenüberwachung und das Recht auf Schutz der Privatsphäre

70. Im Juli 2014 reichten Amnesty International, Liberty, Privacy International, die American Civil Liberties Union und mehrere andere nicht im Vereinigten Königreich ansässige Gruppen beim Investigatory Powers Tribunal eine Anfechtungsklage gegen das Tempora-Programm ein mit der Begründung, dass die mit diesem Programm durchgeführte „Massenüberwachung" illegal ist, und dass die britischen Nachrichtendienste, indem sie Informationen von der NSA beziehen, die vom britischen Rechtssystem gewährten Schutzmechanismen ausgehebelt haben. Wie weiter oben ausgeführt (s. oben Abs. 8-9), weigert sich die Regierung immer noch, die Existenz des Tempora-Programms zu bestätigen bzw. zu dementieren.

71. Im Dezember 2014 urteilte das IPT, dass das britische Rechtssystem im Hinblick auf die Massenüberwachung grundsätzlich rechtmäßig ist. Die Entscheidung des Tribunals beruhte auf vormals geheimen internen Regeln für den Datenaustausch mit den USA, zu deren Offenlegung die Regierung im Laufe der Verhandlungen (die allerdings unter Ausschluss der Öffentlichkeit stattfanden; den Antragstellern wurden Beschreibungen geliefert) gezwungen war. Dies warf jedoch die Frage auf, ob das Überwachungssystem der Regierung vor diesen Offenlegungen im Einklang mit dem Gesetz gehandelt habe, und in einem zweiten Urteil im Februar 2015 befand das Tribunal, dass der Nachrichtenaustausch zwischen den Vereinigten Staaten und dem Vereinigten Königreich vor Dezember 2014 unrechtmäßig gewesen sei. Das war das erste Mal in seiner 15-jährigen Geschichte, dass das IPT eine Entscheidung gegen die Nachrichten- und Sicherheitsdienste fällte.

72. Die Antragsteller sind nunmehr mit einen gemeinsamen Antrag an den Europäischen Gerichtshof für Menschenrechte in Berufung gegen das erste Urteil des IPT vom Dezember 2014 gegangen. Amnesty behauptet: „Der Regierung ist es gelungen, sich mit Blufftaktiken aus der Affäre zu ziehen, sich hinter geschlossenen Anhörungen zu verschanzen und ständig die Karte „nationale Sicherheit" zu spielen. Das Tribunal hat diesen Ansatz akzeptiert. Wir mussten einer aggressiv resistenten Regierung jedes Detail mit viel Akribie und Geduld entlocken... Die gesamte Verteidigung der Regierung lautete stets: „Sie können uns vertrauen", und jetzt hat das Tribunal das Gleiche gesagt."[59] Der Berufungsprozess wird wahrscheinlich zusammen mit einer separaten Anfechtungsklage gegen die britischen Massen-

[59] "UK court decision on government mass surveillance: 'Trust us' isn't enough", Amnesty, 5. Dezember 2014, verfügbar unter: https://www.amnesty.org/en/latest/news/2014/12/uk-court-decision-government-mass- surveillance-trust-us-isnt-enough/.

überwachungsprogramme seitens Big Brother Watch, Open Rights Group, English PEN und der deutschen Aktivistin Constanze Kurz stattfinden, ein Prozess, der zurzeit beim ECHR beschleunigt zur Verhandlung kommen soll. Diese Gruppen entschieden sich dafür, das IPT zu umgehen, weil es „eine Schöpfung genau desjenigen gesetzlichen Systems ist, das versagt hat und kein wirksames Rechtsmittel anbieten könnte".[60]

73. Das Urteil steht zurzeit bei der richterlichen Überprüfung des 2014 Data Retention and Investigatory Powers Act (s. oben, Abs. 24-27) durch den High Court an, die im Juni 2015 stattfand, nachdem eine Beschwerde von den Abgeordneten David Davis und Tom Watson, vertreten durch Liberty, eingereicht worden war. Der Fall hat weitgehend die gleichen materiellrechtlichen Grundlagen wie die erfolgreiche Anfechtungsklage gegen die EU-Richtlinie zur Vorratsdatenspeicherung beim Europäischen Gerichtshof. Der Anwalt der Abgeordneten sagte: „Die Bedenken [der Mandanten] sind, dass dieses Gesetz nicht die notwendigen Mindestvorkehrungen zum Schutz vor dem Risiko willkürlicher, unverhältnismäßiger oder missbräuchlicher Speicherung und Nutzung personenbezogener Daten bietet, und es damit das Grundrecht auf die Privatsphäre verletzt". Davis hat sich verächtlich zu der Art und Weise geäußert, wie das Gesetz „in einer lächerlichen und unnötigen Eile durch das Unterhaus gepeitscht wurde, um einem vollkommen künstlichen Notstand Rechnung zu tragen. Daher hatten die Abgeordneten keine Möglichkeit, entweder Nachforschungen darüber anzustellen, sich Gedanken darüber zu machen oder ordnungsgemäß darüber zu debattieren, und der Zweck dieser Gerichtsklage ist, die Regierung dazu zu zwingen, dem Parlamentshaus das zu ermöglichen, was es ihm von vornherein hätte erlauben müssen: Ordnungsgemäße, gut durchdachte und wirksame Gesetzgebung".[61]
74. Im Juni 2015 wurde die Nutzung von „Massenpersonendatensätzen" durch das GCHQ erstmals angefochten, als Privacy International eine Rechtsbeschwerde beim Investigatory Powers Tribunal einreichte. Die entsprechenden inländischen Befugnisse in den USA (nach Section 215 des PATRIOT Act) waren erst wenige Tage davor durch die Verabschiedung des USA Freedom Act eingeschränkt worden. Privacy International reagierte damit auf den Bericht des Intelligence and Security Committee vom März 2015, der Enthüllungen darüber enthielt, dass kein ordnungsgemäßes Regularium für die Erfassung und anschließende Nutzung von Datensätzen besteht. Für den Zugriff ist keine richterliche oder ministerielle Genehmigung erforderlich, und es gibt auch keine rechtlichen Strafen für den Missbrauch. Privacy International konstatiert: „Der Tatbestand, dass Unternehmen heimlich angewiesen werden, ihre Unterlagen pauschal zu übergeben, sodass die Daten willkürlich ohne unabhängige Genehmigung oder Aufsicht ausgewertet werden können, ist ein riesengroßes Schlupfloch im Gesetz. Die Nutzung dieser Datenbanken, von denen manche freiwillig zur Verfügung gestellt, manche gestohlen und manche durch Erpressung oder Nötigung erlangt wurden, stellt bereits einen Missbrauch dar und wird es bleiben, bis die Praktiken komplett saniert und ordnungsgemäße Schutzmechanismen vorhanden sind."[62]

---

[60] "Privacy not Prism", verfügbar unter: https://www.privacynotprism.org.uk/.

[61] "Two MPs to sue government over data law 'stitch-up'", Channel 4 News, 22. Juli 2014, verfügbar unter: http://www.channel4.com/news/data-drip-law-surveillence-tom-watson-david-davis-legal-sue.

[2] Press Release, Privacy International, 8. Juni 2014, verfügbar unter: https://www.privacyinternational.org/?q=node/594.

„Hacking"

75. Privacy International hat auch zwei separate Beschwerden beim IPT wegen Hacking-Angriffen oder „Ausbeutung von Computernetzwerken" seitens des GCHQ eingereicht. Diese und andere NRO sind besorgt, dass Hacking-Angriffe noch invasiver sind als andere von Snowden enthüllte Überwachungs- oder Datenerfassungsformen, weil sie den Zugriff auf potenziell immense Mengen an personenbezogenen Daten ermöglichen, der sonst nicht gegeben wäre. Das Abfangen von Mitteilungen kann nur das offenlegen, was eine Einzelperson zum Ausdruck bringen wollte; Hacking-Angriffe hingegen ermöglichen es den Nachrichtendiensten, Material zu sehen, das vielleicht niemals freiwillig offengelegt worden wäre. Sogar noch invasiver ist, dass das GCHQ Anwendungen wie eine Kamera, ein Mikrofon oder ein globales Positionierungssystem aktivieren kann, um Inhalte ohne das Wissen oder die Erlaubnis des Eigentümers zu erzeugen, weil dabei heimlich die Kontrolle über einen Rechner oder ein mobiles Gerät erlangt wird. Hacking-Angriffe stehen auch im Mittelpunkt von Bemühungen der Nachrichtendienste, Verschlüsselungsprotokolle zu knacken oder zu umgehen, eine Praxis, die Tim Berners-Lee, Erfinder des World Wide Web und Gründungsdirektor der World Wide Web Foundation, „entsetzlich und dumm" nennt, weil sie wahrscheinlich „kriminellen Hackerbanden und feindlichen Staaten zugute kommt". Berners-Lee betont, dass er „große Sympathie für Bemühungen zur Erhöhung der Sicherheit gegen organisierte Kriminalität empfindet, aber man muss sich von dem Kriminellen unterscheiden".[63]

76. Die erste Beschwerde von Privacy International im Mai 2014 ist eine Anfechtungsklage gegen die „umfangreichen und zudringlichen" Hacking-Aktivitäten des Dienstes in Bezug auf PCs und Geräte. Die von Snowden offengelegten Dokumente enthüllten, dass das GCHQ, oftmals in Parterschaft mit der NSA, „potenziell Millionen von Rechnern und Mobilfunkgeräten weltweit mit schädlicher Software infiziert hat, die den Ermittlern die Möglichkeit gibt, tonnenweise Inhalte zu erfassen, die Mikrofone oder Kameras der Anwender einzuschalten, ihre Telefonate abzuhören und ihre Standorte zu verfolgen."

77. Die zweite Beschwerde von Privacy International wurde im Juli 2014 zusammen mit sieben internationalen Kommunikationsdienstanbietern - Riseup (USA), GreenNet (Vereinigtes Königreich), Greenhost (Niederlande), Mango (Simbabwe), Jinbonet (Korea), May First/People Link (USA) und dem Chaos Computer Club (Deutschland) – gegen die zum Zweck einer massenhaften invasiven Überwachung vom GCHQ betriebene Ausbeutung der KDA-Netzwerkinfrastruktur eingereicht. Die weitverbreitete Art dieser Angriffe wurde in einer Reihe von Artikeln in Der Spiegel und The Intercept dokumentiert. Sie enthüllten, dass das GCHQ über eine Reihe von Möglichkeiten zur Ausbeutung von Netzwerken und zum Eindringen in Netzwerke verfügt, die gezielt gegen eine Reihe von KDA, darunter auch den belgischen Telekommunikationsgiganten Belgacom und Internetknoten von drei deutschen Unternehmen, nämlich Stellar, Cetel und IABG, zum Einsatz kamen.

78. In jeder Beschwerde konstatiert Privacy International, dass die Aktivitäten des GCHQ sowohl nach dem Computer Misuse Act von 1990 (der das Hacking kriminalisiert) als auch nach Artikel 8 und 10 der Europäischen Menschenrechtskonvention, die verlangen, dass jeder Eingriff in die Privatsphäre und in die Meinungsfreiheit durch einen eindeutigen rechtlichen Rahmen reglementiert werden müssen, um vor Machtmissbrauch und Willkür zu schützen, illegal ist. Da das GCHQ nicht die rechtliche Grundlage für seine Hacking-Aktivitäten offengelegt hat, ist Privacy International davon ausgegangen, dass die Rechtfertigung durch inländisches Recht auf einer nach Section 5 des Intelligence Services Act 1994 ergangenen Anordnung beruht, die den „Zutritt oder Eingriff in Eigentum oder mit drahtloser Telegrafie" unter bestimmten Bedingungen zulässt, und in Fällen von Hacking-Angriffen außerhalb des Vereinigten Königreichs auf einer Anordnung nach Section 7 des Gesetzes, die Straffreiheit verspricht für „jede

[63] "Tim Berners-Lee: encryption cracking by spy agencies 'appalling and foolish'", Guardian, 6. November 2013, verfügbar unter: http://www.theguardian.com/world/2013/nov/06/tim-berners-lee-encryption-spy-agencies.

Handlung außerhalb der Britischen Inseln, wenn die Handlung aufgrund einer durch den Secretary of State nach Maßgabe dieses Abschnitts erteilte Genehmigung genehmigt wurde...".[64]

79. Im Mai 2015, am Tag vor der geplanten Anhörung der zweiten Beschwerde von Privacy International vor dem IPT, enthüllte die Regierung in ihren rechtlichen Akten, dass der Computer Misuse Act umgeschrieben worden war, um Justizvollzugs- und Nachrichtendienste von der strafrechtlichen Haftung für Hacking-Angriffe zu befreien. Das Gesetz war durch eine scheinbar kleinere „klärende Änderung" des Gesetzentwurfs über Schwerverbrechen geändert worden, der am 3. März 2015 von der Königin genehmigt wurde und am 3. Mai 2015 in Kraft trat. Privacy International reagierte folgendermaßen: „Die das Gesetz begleitenden erklärenden Kommentare enthalten keinerlei Hinweis auf die wahren Auswirkungen der Änderung. Offenbar wurden weder Regulierungsbehören noch die für die Beaufsichtigung der Nachrichtendienste zuständigen Kommissare, das Information Commissioner's Office, die Branche, die NRO oder die Öffentlichkeit bezüglich der vorgeschlagenen legislativen Änderungen benachrichtigt oder zu Rate gezogen. Es wurde keine Folgenabschätzung für die Privatsphäre veröffentlicht. Nur das Justizministerium, der Crown Prosecution Service, das Scotland Office, das Northern Ireland Office, das GCHQ, die Polizei und die National Crime Agency wurden als Interessengruppen zu Rate gezogen. Es fand keine öffentliche Debatte statt."[65]

80. Die Regierung hatte mit der Veröffentlichung eines Entwurfs für einen Verhaltenskodex, den „Equipment Interference Code of Practice", im Februar 2015 bereits auf Behauptungen reagiert, die Hacking-Aktivtäten des GCHQ würden gegen die ECHR-Erfordernisse für klare formalrechtliche Richtlinien verstoßen.[66] Der Entwurf des Kodex, auf den sich die Regierung in ihrer offenen Antwort gegenüber den zwei IPT-Fällen massiv berufen hat, spiegelt offenbar die internen Richtlinien des GCHQ wider. Der Entwurf unterlag einer sechswöchigen öffentlichen Beratung, deren Ergebnisse zurzeit ausgewertet werden. Die Regierung weigerte sich, die früheren Versionen des Kodex des GCHQ oder das Datum seiner Erstfassung gegenüber Privacy International offenzulegen und berief sich dabei auf Bedenken wegen der nationalen Sicherheit.[67] Mit dem Entwurf des Kodex werden erstmals die Umstände und Verfahren im Rahmen der Computernetzwerkausbeutung veröffentlicht und wird bestätigt, dass die Nachrichtendienste erhebliche Befugnisse zum Hacken von PCs und Telefonen besitzen und Kommunikationsnetzwerke überall in der Welt ausbeuten können, selbst wenn die Zielperson nicht als Bedrohung der nationalen Sicherheit wahrgenommen oder verdächtigt wird, eine Straftat begangen zu haben. Die Regierung wurde von prominenten Akademikern für ihren Versuch kritisiert, ein Gesetz über hochinvasive Praktiken mit minimaler demokratischer Prüfung über einen Verhaltenskodex statt über das Primärrecht der Legislative in Kraft zu setzen (s. Abs. 96-97).[68]

Informationsfreiheit und Vereinbarungen zum Nachrichtenaustausch

81. Der Europäische Gerichtshof für Menschenrechte hat auch eine Anfechtungsklage zugelassen, die im September 2014 von Privacy International wegen der pauschalen Befreiung des GCHQ vom britischen Freedom of Information Act eingereicht wurde. Privacy International konstatiert, dass es den Nach-

---

[64] Begründung, verfügbar unter: https://www.privacyinternational.org/sites/default/files/Final%20Grounds%20-%20GCHQ%20attacking%20providers 0.pdf.

[65] Pressemitteilung, Privacy International, 15. Mai 2014, verfügbar unter: https://www.privacyinternational.org/?q=node/584.

[66] "Draft Equipment Interference Code of Practice", 6. Februar 2005, verfügbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/401863/Draft Equipment I nterference Code of Practice.pdf.

[67] s. o., Fußnote 65.

[68] "Snowden slams UK government attempts to secretly pass legislation allowing GCHQ to 'hack anybody's computer'", computing.co.uk, 2. Juni 2015, verfügbar unter: http://www.computing.co.uk/ctg/news/2411261/snowden-slams-uk-government-attempts-to-secretly-pass-legislation-allowing-gchq-to-hack-anybodys-computer.

richtendiensten nicht gestattet werden darf, Vereinbarungen über den Datenaustausch mit andern Ländern geheimzuhalten, und dass es im öffentlichen Interesse ist, das GCHQ zur „Veröffentlichung von Dokumenten zu verpflichten, in denen aufgeführt wird, wie die Überwachungsdaten mit den Five-Eyes-Partnern, darunter auch die NSA, ausgetauscht bzw. von diesen beschafft werden".[69]

Schutz von Journalisten, Rechtsanwälten und NRO

82. Das ECHR hat ein beschleunigtes Verfahren für einen Fall eingeleitet, der im September 2014 vom Bureau of Investigative Journalism über den Mangel an Schutz durch die britische Gesetzgebung für Journalisten und ihre Quellen vor Massenüberwachungs- und Abhörprogrammen eingereicht worden war. Das Gericht wurde aufgefordert, über die Angemessenheit rechtlicher Schutzmechanismen im RIPA gegen unberechtigte Überwachung durch alle relevanten Behörden zu befinden. RA Gavin Millar (QC) stellte auftrags der Rechtsanwälte des TIBJ fest, dass „die Polizei gegenwärtig die Befugnisse zur verdeckten Ermittlung nach dem RIPA routinemäßig missbraucht, um an die Metadaten von Journalisten zu gelangen und damit ihre Quellen zu identifizieren. Dies unterläuft die Rechte eines Journalisten, eine Informationsquelle zu schützen, und seine Rechte auf eine Anhörung vor einem Richter, bevor eine Anweisung zur Offenlegung solcher Informationen ergeht. Die schiere Menge an Daten, die vom GCHQ nach dem RIPA erfasst wird, bedeutet, dass Sicherheits- und Nachrichtendienste auch ständig verdeckt auf vertrauliches journalistisches Material zugreifen und es analysieren. Auch hier werden die Quellen identifiziert – aber in viel größerem Maßstab. Dennoch steht kein Wort über diese wichtigen Rechte von Journalisten im RIPA oder im Verhaltenskodex der Regierung. Das Vereinigte Königreich ignoriert die Konvention einfach."[70]

83. Wie bereits oben erwähnt, veröffentlichte die Regierung nach früheren Beschwerden von Amnesty und Reprieve beim Intelligence Powers Tribunal wegen der Überwachung von Kommunikationen zwischen Anwälten und ihren Mandanten (s. oben, Abs. 30-31) Entwürfe von „Verhaltenskodexen" für die staatliche Überwachung vertraulicher Kommunikationen zwischen Rechtsanwälten, Journalisten, Abgeordneten und Mitgliedern der Öffentlichkeit. Nach Kat Craig, Chefsyndikus von Reprieve, haben die Vorschläge „kläglich versagt, eine Ausgewogenheit zwischen Sicherheit und Privatsphäre herzustellen.[71] Bestenfalls decken sie die Unfähigkeit der Regierung auf, die Risiken moderner Überwachungsbefugnisse zu verstehen. Schlimmstenfalls deuten sie auf einen bedrohlicheren Widerstand hin, sich an rechtsstaatliche Grundsätze zu halten. Natürlich spielt die Überwachung eine entscheidende Rolle in der Sicherheit unserer Nation, aber das kann genauso gut mit entsprechenden Sicherheitsmechanismen geschafft werden – etwas, was diese Vorschläge eindeutig nicht bieten."

84. Im Juni 2015 stellte das IPT Verfahrensfehler bei der Überwachung zweier internationaler NRO durch das GCHQ fest. Auffällig ist, dass das Tribunal nicht die Überwachung selbst für illegal befand, sondern das Versagen des GCHQ, seine eigenen geheimen internen Regeln zu befolgen, wurde als Rechtsverletzung gewertet.[72] Im Fall der ägyptischen Initiative für Persönliche Rechte wurde festgestellt, dass Kommunikationen „wesentlich länger als nach den GCHQ-Richtlinien zulässig" aufbewahrt wurden. Und beim südafrikanischen „Legal Resources Centre" wurde das Verfahren zur Auswahl zu analysierender Kommunikationen „fälschlicherweise nicht eingehalten". Die zwei Gruppen gehörten zu einem großen NRO-Konsortium, das eine Klage gegen die [britische] Regierung eingereicht hatte. Das IPT

---

[69] "Privacy International v. United Kingdom" , verfügbar unter: https://www.privacyinternational.org/?q=node/83.

[70] "Bureau files ECHR case challenging UK government over surveillance of journalists' communications", The Bureau of Investigative Journalism, 14. September 2014, verfügbar unter: https://www.thebureauinvestigates.com/2014/09/14/bureau-files-echr-case-challenging-uk-government-over-surveillance-of-journalists-communications/.

[71] "Government's new lawyer-snooping guidance "fails dismally"", Reprieve, 20. März 2015, verfügbar unter: http://www.reprieve.org.uk/press/governments-new-lawyer-snooping-guidance-fails-dismally-reprieve/.

[72] "GCHQ intercepts communications of human rights groups", Liberty, 22. Juni 2015, verfügbar unter: https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/gchq-intercepts- communications-human-rights-groups.

stellte fest, dass das GCHQ nicht verantwortlich war, den anderen Antragstellern – darunter Amnesty International, Liberty und Privacy International – Rede und Antwort zu stehen, und legte daher auch nicht offen, ob diese Organisationen überwacht worden waren. Aufgrund von Bedenken wegen der nationalen Sicherheit weigerte das Tribunal sich auch offenzulegen, warum es für notwendig und angemessen befunden wurde, dass das GCHQ die ägyptische Initiative für Persönliche Rechte und das südafrikanische Legal Resources Centre ausspioniert hat. Grundsätzlich jedoch akzeptierte das IPT, dass die britischen Nachrichtendienste ein gesetzliches Recht zur Überwachung ausländischer Bürgerrechts-NRO haben.

VI ZIVILGESELLSCHAFTLICHE KAMPAGNEN

85. Dieser Abschnitt erklärt die öffentlichen Positionen wichtiger Akteure aus der „bürgerlichen Gesellschaft" im Hinblick auf die Auswirkungen und Reformen der Überwachungspolitik und -praxis. Er enthält Stellungnahmen von NRO, Akademikern und Berufsverbänden.

'Don't Spy On Us'

86. Die Kampagne 'Don't Spy On Us' – eine Koalition aus britischen und internationalen Bürgerrechtsgruppen einschließlich Liberty, ARTICLE19, Big Brother Watch, English PEN, Open Rights Group und Privacy International – wurde im Februar 2014 als gemeinsame Opposition gegenüber die „ungehinderte Massenüberwachung durch den Staat" gebildet.[73]

87. Die Kampagne und ihre Mitglieder haben sich sehr kritisch zu den Berichten des Intelligence and Security Committee des Parlaments, insbesondere seiner Feststellung, dass sich das GCHQ nicht an der „Massenüberwachung beteiligt", geäußert (s. oben, Abs. 44-52). „Wie kann man denn sonst das Filtern von Milliarden an Kommunikationen und die Durchsuchung dieser Kommunikationen mit zehntausenden Selektoren bezeichnen?", lautete die Frage.[74] „Selbst mit noch so viel technischem und juristischem Jargon lässt sich nicht die Tatsache verheimlichen, dass es sich hier um einen parlamentarischen Ausschuss handelt, in einem demokratischen Land, der seinen Bürgerinnen und Bürgern sagt, dass sie in einem Überwachungsstaat leben und alles in Ordnung ist", entgegnete Privacy International.[75]

88. Umgekehrt begrüßten die NRO generell die vom Independent Reviewer of Terrorism Legislation (s. oben, Abs. 62-68) durchgeführte Überprüfung und die „offene Art und Weise, mit der er den durch die Snowden-Dokumente enthüllten Wahrheiten über einen Überwachungsexzess gegenübertritt – ein Novum bei amtlichen Berichten oder Überprüfungen im Vereinigten Königreich, seit die Enthüllungen vor zwei Jahren begannen."[76] Liberty befand, dass sein „gut durchdachter, sinnvoller Bericht... der Anfang eines Neuaufbaus des öffentlichen Vertrauens in eine mit Respekt für die Privatsphäre, die Demokratie und das Gesetz durchgeführte Überwachung sein könnte."[77] Die Vertreter von Liberty drückten jedoch ihre Enttäuschung aus, dass sich Anderson bei seiner Empfehlung einer Distanzierung von willkürlichen Unterscheidungen zwischen „internen" und „externen" Kommunikationen nicht gegen diskriminierende Schutzmechanismen für die Privatsphäre aussprach, nach denen britische Staatsbürger und Einwohner mehr Rechte genießen als Ausländer: „Seine Empfehlungen verankern

---

[73] "Don't Spy On Us", verfügbar unter: https://www.dontspyonus.org.uk/.

[74] "UK Parliament's Intelligence Committee says reform needed after Snowden revelations", Don't Spy On Us, März 2015, verfügbar unter: https://www.dontspyonus.org.uk/blog/2015/03/12/uk-parliaments-intelligence- committee-says-reform-needed-after-snowden-revelations/.

[75] Press Release, Privacy International, 12. März 2015, verfügbar unter: https://privacyinternational.org/?q=node/505.

[6] Pressemitteilung, Privacy International, 11. Juni 2015, verfügbar unter: https://www.privacyinternational.org/?q=node/595.

[77] "Undemocratic, unnecessary and - in the long run - intolerable": Government reviewer condemns Britain's snooping laws", Liberty, 11. Juni 2015, verfügbar unter: https://www.liberty-human-rights.org.uk/news/press- releases-and-statements/%E2%80%9Cundemocratic-unnecessary-and-%E2%80%93-long-run-%E2%80%93- intolerable%E2%80%9D.

die Haltung der Regierung, dass die Massenüberwachung von Ausländern eine akzeptable Aktivität für einen demokratischen Staat ist, und verbessern den Schutz für Briten, während sie Eingriffe in die Privatsphäre aller anderen untermauern."[78]

89. Die Kampagne Don't Spy On Us gibt 13 konkrete Empfehlungen für die Überwachungsreform im Vereinigten Königreich: (i) Die Gesetze RIPA und DRIPA sind aufzuheben und durch eine neue, umfassende Gesetzgebung zu ersetzen; (ii) Alle Überwachungsentscheidungen (auch das Abfangen von Kommunikationan und der Zugriff auf Kommunikationsdaten) müssen einer vorherigen richterlichen Genehmigung unterliegen; (iii) Das Abfangen von Kommunikationen muss stets gezielt und konkret statt massenhaft und wahllos erfolgen; (iv) Für Kommunikationsdaten sollte der gleiche Schutz gelten wie für den Inhalt von Kommunikationen. Die Speicherung von Metadaten sollte ebenfalls gezielt und konkret erfolgen; (v) Die Überwachung sollte nur für Zwecke durchgeführt werden, die präziser und enger definiert sind, als es bislang der Fall ist; (vi) Die Regierung sollte davon absehen, Verschlüsselungsstandards zu brechen und die Sicherheit im Internet zu unterminieren. Diese Aktivität sollte explizit durch die Gesetzgebung verboten sein; (vii) Internationale Vereinbarungen, die die Erfassung und den Austausch der Überwachungsergebnisse regeln, müssen publik gemacht und parlamentarischer und richterlicher Aufsicht unterzogen werden, und sollten es Einzelpersonen ermöglichen vorherzusehen, wann es wahrscheinlich ist, dass sie überwacht werden. Dieses Erfordernis sollte gesetzlich festgelegt werden; (viii) Die Regierung sollte zusammenfassende Informationen über die Anzahl von genehmigten bzw. abgelehnten Anträgen auf Überwachungsaktionen veröffentlichen, um die Transparenz zu verbessern; (ix) Für den illegalen Zugriff auf Kommunikationsdaten und die unbefugte Nutzung anderer Überwachungstechniken sollten geeignete Rechtsbehelfe zur Verfügung stehen; (x) Das Investigatory Powers Tribunal sollte eine offenere und gerechtere Verfahrensweise pflegen. Folgendes sollte dazugehören: Anhörungen; öffentliche Anhörungen, wenn die Regierung nicht nachweist, dass in dem konkreten Fall eine geheime Behandlung erforderlich ist; Nachweise sollten offengelegt und Urteile sowie ihre Begründungen veröffentlicht werden, es sei denn, die Regierung weist nach, dass eine geheime Behandlung erforderlich ist; spezielle Juristen sollten ernannt werden; für Gerichtsbeschlüsse sollten Berufungs- bzw. Revisionsbefugnisse gelten;Das Intelligence and Security Committee sollte einer Reform unterzogen werden, sodass das Gremium: unmittelbar gegenüber dem Parlament rechenschaftspflichtig ist; befugt ist, Beschlüsse über Berichtswesen und Veröffentlichung zu fassen; und angemessen mit Mitteln und Personal ausgestattet ist. Es sollte stärkere Befugnisse zur Erzwingung von Informationsbeschaffung und Zeugenaussagen haben. Der/die Vorsitzende sollte Mitglied der größten Oppositionspartei sein, und die Mitglieder im House of Commons sollten gewählt und nicht durch die Fraktionsführer ernannt werden;

(xi) Der Intelligence Services Commissioner und der Interception of Communications Commissioner sollten mit adäquaten Mitteln ausgestattet sein, dem Parlament unterstellt sein und eine viel größere Anzahl an Datenanträgen überprüfen; (xiii) In Strafrechtsverfahren sollten durch Abfangen erlangte Beweismittel zulässig sein.[79]

„Öffnung der Five Eyes"

90. Nach den Snowden-Enthüllungen startete die Londoner Bewegung Privacy International die Kampagne „Eyes Wide Open" mit der Zielsetzung, die Five-Eyes-Vereinbarung aufzubrechen und sie in den Bereich eines rechtsstaatlichen Systems zu bringen.[80] Die Kampagne betont das Integrationsniveau zwischen den britischen und amerikanischen Nachrichtendiensten und führt Zitate von Mitgliedern der Nachrichtendienste an, die gesagt haben, dass die Zusammenarbeit nach dem UK-USA-Abkommen so vollständig ist, dass „es sehr schwierig wird, zu ermitteln, wer genau was macht [...] es ist einfach ein organisatorisches Chaos." Ein weiteres führendes Mitglied der britischen Nachrichtendienste wird zitiert mit den Worten „Wenn man einen GCHQ-Pass bekommt, dann hat man auch den Zugang zur

[78] Press Release, Privacy International, 11. Juni 2015, verfügbar unter: https://www.privacyinternational.org/?q=node/596.

[79] "Reforming surveillance in the UK", Don't Spy On Us, September 2014, verfügbar unter: https://www.dontspyonus.org.uk/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf.

[80] "Eyes Wide Open", Privacy International, verfügbar unter: https://www.privacyinternational.org/?q=node/42.

NSA. Man kann in die NSA hineinspazieren und dabei entdecken, dass GCHQ-Mitarbeiter in führenden Positionen arbeiten, und umgekehrt.

91. Der Start der Kampagne „Eyes Wide Open" wurde begleitet von der Veröffentlichung eines Berichts, nach dem „Das Flickwerk an geheimen Spionageprogrammen und Vereinbarungen zum Nachrichtenaustausch, das von den Parteien der „Five Eyes"-Vereinbarung eingeführt wurde, eine integrierte, globale Überwachungsmaßnahme" darstellt, „die nunmehr die Mehrzahl der Kommunikationen weltweit abdeckt."[81] In dem Bericht wird die Forderung zur Würdigung einer „interventionsbasierten Justiz" gestellt, die „die Art und Weise, wie die globale Kommunikationsinfrastruktur aufgebaut ist", widerspiegelt und „es ermöglicht, dass das Recht auf Schutz der Privatsphäre weltweit ausgeübt werden kann."

Berufsverbände und Gewerkschaften

92. Berufsverbände als Vertretungsorgane von Rechtsanwälten und Journalisten haben starke Kritik an den von Snowden enthüllten Überwachungspraktiken und mehrfach Bedenken wegen ihrer Folgen für ihre Mitglieder geäußert. [Anm. d. Übers.: Fehler im englischen Ausgangstext]

93. „Der Whistleblower Edward Snowden hat die Angehörigen freier Berufe, darunter auch Rechtsanwälte, dazu aufgerufen, ihre Sicherheitsvorkehrungen nach den Überwachungsenthüllungen zu verbessern", teilte die britische Anwaltskammer ihren Mitgliedern nach den ersten Offenlegungen mit;[82] dabei forderte sie eine „öffentliche Debatte zum Thema Überwachung."[83] Der Präsident der Anwaltskammer erklärte: „Ich werde den Vertretern anderer Berufsverbände schreiben, damit wir die Folgen der Spionage für die vertraulichen Kommunikationen unserer Mitglieder mit ihren Mandanten oder Patienten diskutieren können. Ich werde auch relevante Akademiker, Bürgerrechtsgruppen, Anwälte und andere Fachleute sowohl im Vereinigten Königreich als auch im Ausland anschreiben und sie einladen, mit uns bei der Behandlung breiterer Fragen bezüglich Überwachung und Rechtsstaat zusammenzuarbeiten." Eine Pressemitteilung der Anwaltskammer als Reaktion auf die im Jahr 2014 verabschiedeten ‚Notstandsbestimmungen' zur Datenspeicherung enthielt folgende Aussage: „Unsere Sorge über die möglichen Folgen der Gesetzgebung zur Vorratsdatenspeicherung (Data Retention and Investigatory Powers law), die von der Regierung in dieser Woche im Eiltempo durch das Parlament geschleust wurde, könnte kaum größer sein." Die Anwaltskammer forderte Reformen „zur Vereinfachung und Klärung eines komplexen und verwirrenden rechtlichen Rahmens, um sicherzustellen, dass er die Menschenrechte schützt."[84]

94. Die National Union of Journalists (NUJ) äußerte sogar noch heftigere Kritik an den Überwachungsbefugnissen und unterstützte die Whistleblower, Journalisten und den Schutz ihrer Quellen, gab zahlreiche Erklärungen ab, veranstaltete Konferenzen und bot ihren Mitgliedern kostenlose Schulung über den Schutz der Privatsphäre und Informationssicherheit an.[85] Im April 2014 verabschiedete die NUJ einen Antrag zur Gründung einer Kommission zur Beurteilung neuer Gesetze zum Schutz von Personen und Organisationen gegen unnötige Überwachung durch den Staat.[86]

---

[81] "Eyes Wide Open: Special Report", Privacy International, 26. November 2013, verfügbar unter: https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf.

[82] "Cyber security", Law Society, verfügbar unter: http://www.lawsociety.org.uk/support-services/practice- management/cyber-security/.

[83] "Law Society backs public debate on surveillance issues", 18. Juli 2014, verfügbar unter: http://www.theguardian.com/world/2014/iul/18/law-society-debate-surveillance.

[84] "Stark warning on emergency surveillance legislation", Law Society, 10. Juli 2014, verfügbar unter: http://www.lawsocietv.org.uk/news/press-releases/stark-warning-on-emergency-surveillance-legislation/.

[5] NUJ website, verfügbar unter: https://www.nuj.org.uk/site-search/?&keywords=snowden&p=2.

[86] "DM2014: Orwell's worst dream", NUJ, 12. April 2014, verfügbar unter: https://www.nuj.org.uk/news/dm2014- orwells-worst-dream/.

95. Die NUJ legte auch eine Petition vor, die beim Trades Union Congress (der britischen Föderation von Gewerkschaften) im Jahr 2013 mit überwältigender Mehrheit angenommen wurde. In der Petition heißt es: „Der Congress ist besonders besorgt wegen der von Edward Snowden, der früher für die NSA der USA tätig war, enthüllten beispiellosen, von industrieähnlichen Bedingungen geprägten geheimen Datenerfassung und Internetüberwachung von Millionen Bürgern, darunter auch Briten, durch NSA und GCHQ. Der Congress glaubt, dass der Schutz der Privatsphäre, ganz abgesehen von der Notwendigkeit, einen rechtlichen Schutzschild für Whistleblower zu gewährleisten, eindeutig im öffentlichen Interesse ist, besonders im Bereich Informationsfreiheit."[87]

Die akademische Welt

96. Im Mai 2015 veröffentlichte eine Gruppe von 38 im Vereinigten Königreich ansässigen Akademikern ein offenes Schreiben an die Abgeordneten mit der dringenden Forderung an die neue Regierung, „sicherzustellen, dass etwaige Gesetzesänderungen und insbesondere auch Befugniserweiterungen vollumfänglich und transparent vom Parlament genehmigt werden und eine Konsultation der Öffentlichkeit und aller relevanten Interessengruppen möglich ist."[88] Manche der Unterzeichner hatten auch eine internationale Erklärung mit dem Titel „Academics Against Mass Surveillance" unterzeichnet, die im Januar 2014 veröffentlicht wurde.[89] Manche hatten auch im Juli an die Regierung geschrieben und verlangt, dass der damalige Gesetzentwurf, die Data Retention and Investigatory Powers Bill, einer vollständigen und rigorosen parlamentarischen Kontrolle unterliegen sollte, weil er „eine ernsthafte Erweiterung des britischen Überwachungsstaates darstellt". Insbesondere protestierten sie gegen die Darstellung der Gesetzgebung durch den Innenminister als bloße Bestätigung des vorher bestehenden britischen Datenspeicherungssystems, wohingegen es die Ermittlungsbefugnisse tatsächlich bedeutend erweiterte (s. oben, Abs. 26).

97. In dem Schreiben vom Mai 2015 heißt es, dass diese laxe Haltung gegenüber ordnungsgemäßen Verfahrensregeln weiterhin besteht, und dass die Ermittlungsbefugnisse „auf eine Art und Weise vorgelegt werden, die offenbar beabsichtigt ist, um eine ordentliche demokratische Beurteilung zu vereiteln." Die Unterzeichner kritisieren die Art und Weise, wie die Regierung versuchte, Regeln über das Hacking durch einen Verhaltenskodex statt durch das Primärrecht einzuführen, und die der Polizei und den Nachrichtendiensten gewährte Straffreiheit für Hacking-Aktivitäten durch eine „erläuternde Änderung" des Serious Crimes Act 2015. In der Erwartung, dass die legislative Agenda des neuen Parlaments die Wiederbelebung der Communications Data Bill und eine Überprüfung des RIPA vorsehen wird, fordern die Unterzeichner in dem Schreiben die Regierung auf, die Überwachungsbefugnisse nur über Primärrecht zu erweitern und dabei den in der Europäischen Menschenrechtskonvention verankerten Rechten zum Schutz der Privatsphäre gebührend Rechnung zu tragen. "Es sollte der Regierung nicht erlaubt sein, das Gesetz beliebig und klammheimlich zu ändern, besonders wenn diese Änderungen unsere Privatsphäre und Sicherheit gefährden."

98. Die in Bezug auf das Hacking geäußerten Besorgnisse spiegelten den Inhalt eines offenen Schreibens der University of Bristol Cryptography Group vom September 2013 wider: „Durch die Herabsetzung kryptografischer Standards auf bislang verborgene Art und Weise und den Einbau von Schwachstellen in Produkte, auf die wir uns alle im Interesse des Schutzes einer kritischen Infrastruktur verlassen, haben die [Nachrichten]Dienste nach unserer Meinung gegen die Interessen der Öffentlichkeit gehandelt, denen sie eigentlich dienen sollen. Wir finden es schockierend, dass die Nachrichtendienste so-

---

[87] "Congress backs campaigns on workplace bullying, mass surveillance and to scrap the lobbying bill", NUJ, 13. September 2013, verfügbar unter: https://www.nuj.org.uk/news/congress-backs-campaigns-on-workplace- bullying-mass/.

[88] "Ensuring the Rule of Law and the democratic process is respected as UK surveillance law is revised", Offener Brief an das britische Parlament, 27. Mai 2015, verfügbar unter: http://www.technollama.co.uk/open-letter-to-uk- parliament-about-surveillance.

[89] "Hundreds of academics protest against mass surveillance", Wired, 3. Januar 2014, verfügbar unter: http://www.wired.co.uk/news/archive/2014-01/03/academics-against-mass-surveillance.

wohl der amerikanischen als auch der britischen Regierung nunmehr dafür angeklagt sind, die zu unserem Schutz bestehenden Systeme zu unterminieren. Indem sie unsere gesamte Sicherheit schwächen, um die Kommunikationen unserer Feinde abhören zu können, schwächen sie auch unsere Sicherheit gegenüber unseren potenziellen Feinden. Wir fordern die betreffenden Parteien auf offenzulegen, welche Systeme geschwächt wurden, damit diese wieder repariert werden können, und ein ordentliches Aufsichtssystem mit klar definierten öffentlichen Regeln zu schaffen, welche die Kompromittierung der Sicherheit ziviler Systeme und Infrastrukturen eindeutig verbieten."[90]

99. Es ist auch bemerkenswert, dass das britische Economic and Social Research Council im Oktober 2014 der School of Journalism, Media and Cultural Studies der Cardiff University die Finanzierung eines 18-monatigen Projekts "Digital citizenship and surveillance society: UK state-media-citizen relations after the Snowden Leaks" gewährte, um "die Art, Möglichkeiten und Herausforderungen des digitalen Bürgertums angesichts regierungsseitiger Überwachungsmaßnahmen" zu durchleuchten.[91] Die vorläufigen Feststellungen des Projekts heben die Besorgnisse der Öffentlichkeit wegen des "Mangels an Transparenz über das Niveau der staatlichen Überwachung im Vereinigten Königreich" hervor. „... die Menschen sind sich überaus bewusst, dass eine Online-Überwachung stattfindet, sei es durch den Staat, Unternehmen, Arbeitgeber oder Kollegen... fühlen sich aber auch machtlos, viel daran zu ändern. Diese relative Resignation gegenüber den Realitäten der Massenüberwachung im Vereinigten Königreich steht wohl im Kontrast zu den Entwicklungen, die wir zwei Jahre nach den Snowden-Enthüllungen in Deutschland und den USA beobachten".[92]

100. Und schließlich findet eine bedeutsame und laufende Debatte unter britischen Rechtsgelehrten über die Legitimität und Vereinbarkeit der von Snowden enthüllten Überwachungspraktiken mit dem britischen Gesetz zu den Menschenrechten und entsprechendem internationalem Recht statt.[93] Man kann jedoch fairerweise sagen, dass Debatten über Fragen wie die außerterritoriale Anwendung der britischen Menschenrechtspflichten gegenüber der Signalaufklärung die Fantasie der Öffentlichkeit bislang nicht erreicht haben.

VII DIE BEDEUTUNG DIESER INFORMATIONEN FÜR DEUTSCHLAND

101. Trotz der Unnachgiebigkeit der Regierung, der parlamentarischen Hochachtung für die Nachrichtendienste und der Neigung vieler hochgestellter Personen in den Medien, die Integrität und Motive von Snowden (und der Journalisten, mit denen er zusammenarbeitete) in Frage zu stellen, ist in der öffentlichen Debatte im Vereinigten Königreich ein allmählicher, aber fundamentaler Wandel in Richtung der allgemeinen Erkenntnis zu beobachten, dass eine grundlegende Reform der britischen Überwachungsgesetze nunmehr sowohl notwendig als auch wünschenswert ist. Wie der Independent Reviewer of Terrorism Legislation der Regierung feststellt: „Wir haben jetzt die Gelegenheit, ein von Verwirrung, Verdächtigungen und ständigen Anfechtungsklagen geprägtes System zu nehmen und in einen weltweit erstklassigen Rahmen zur Regulierung starker und lebenswichtiger Befugnisse zu verwandeln".[94]

102. Aber obwohl sich alle Interessengruppen nunmehr der Notwendigkeit einer Reform bewusst sind, ist die Verwirklichung bei einigen Reformen klar wahrscheinlicher als bei anderen. Die Konsolidierung und Vereinfachung des Primärrechts zur Regelung der Aktivitäten der Nachrichtendienste und Überwachungsbefugnisse, insbesondere des „Regulation of Investigatory Powers Act 2000" und der unzähli-

---

[90] "Open Letter From UK Security Researchers", Bristol Cryptography Blog, verfügbar unter: http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html.

[91] "Digital Citizenship and Surveillance Society", DCSS project, verfügbar unter: http://www.dcssproject.net/.

[92] "Edward Snowden's lawyer among prestigious line-up of privacy campaigners, scholars, journalists and tech experts in Cardiff for major surveillance event", Cardiff University, 18. Juni 2015, verfügbar unter: http://www.cardiff.ac.uk/news/view/113535-edward-snowdens-lawver-among-prestigious-line-up-of-privacv- campaigners.-scholars.-journalists-and-tech-experts-in-cardiff-for-maior-surveillance-event.

[93] Siehe z. B. "UK Human Rights Blog" (http://ukhumanrightsblog.com/), "Blog of the European Journal of International Law" (http://www.ejiltalk.org/tag/surveillance/) und "UK Constitutional Law Association" (http://ukconstitutionallaw.org/).

[94] s. o., Fußnote 57.

gen Rechtsakte, Verhaltenskodexe und Aufsichtsmechanismen, welche seine Umsetzung regeln, ist unvermeidbar (die Regierung hat bereits ein umfassendes legislatives Paket versprochen). Es ist auch wahrscheinlich, dass die Vorschläge auf den Trends in Richtung einer erhöhten nachträglichen administrativen und parlamentarischen Aufsicht und statistischen Meldung grundsätzlicher qualitativer Daten zur Überwachung aufbauen werden. Es bleibt jedoch abzuwarten, ob die britische Regierung bereit sein (oder das Parlament fordern) wird, sich in die Nähe des Niveaus an bescheidenen Reformen zu bewegen, die wir bislang in den USA beobachten konnten.

103. Ungeachtet der potenziellen Auswirkungen künftiger Urteile britischer und europäischer Gerichte haben sich die Regierung und die Instanzen, die sie zur Beratung herangezogen hat, weitgehend zufrieden erklärt mit dem von den Nachrichtendiensten praktizierten Überwachungsniveau, mit dem Hinweis, dass eine signifikante Einschränkung ihrer gegenwärtigen Befugnisse und Möglichkeiten unwahrscheinlich ist. In diesem Zusammenhang betrachten die Menschenrechtsorganisationen vorab gefasste richterliche Genehmigungen für Überwachungsaktivitäten als die einzig glaubwürdige Möglichkeit, dafür Sorge zu tragen, dass diese Befugnisse nur dann ausgeübt werden, wenn es notwendig und angemessen ist. Die Regierung hat jedoch auch ihre Absicht signalisiert, die britische Position als einziges Five-Eyes-Land, das über keine Form von richterlicher Vorabgenehmigung von Überwachungsaktivitäten für Internet und Telekommunikation verfügt, aufrechtzuerhalten.

104. Was für Deutschland und tatsächlich auch für den Rest der Welt von entscheidender Bedeutung ist, ist der klägliche Mangel an Debatten im Hinblick auf die Notwendigkeit (oder auch nicht), die Nachrichtenbeschaffungsoperationen des Vereinigten Königreichs einzuschränken. Die Beteiligung der britischen Nachrichtendienste beim Ausspionieren der Regierungen von EU-Partnerländern hat beispielsweise kaum Widerspruch hervorgerufen, abgesehen von den Seiten der Zeitungen, die über die Enthüllungen berichteten. Das liegt teilweise daran, dass die britischen Bürgerrechtsorganisationen versucht haben, den Fokus auf die ‚Massenüberwachung' der allgemeinen Bevölkerung aufrechtzuerhalten, aber es spiegelt auch die Vorstellung wider, dass die Menschen überall im Allgemeinen viel toleranter gegenüber der Überwachung von Ausländern durch Regierung sind.[95]

105. Ein weiteres entscheidendes, aber größtenteils vernachlässigtes Element der Debatte nach Snowden sind die offensiven „Hacking"-Aktivitäten der britischen Nachrichtendienste. Im Zusammenhang mit den von vielen Unternehmen und Privatpersonen weltweit ergriffenen Maßnahmen zum Schutz ihrer Kommunikationen durch Techniken oder Plattformen zum Schutz der Privatsphäre sind diese Aktivitäten recht bedeutend. Gegenwärtig kommen die britischen Nachrichtendienste in den Genuss fast grenzenloser Befugnisse zum straflosen „Hacken" öffentlicher Netzwerke und PCs, und die Regierung hat ihnen kürzlich erhebliche Mittel zukommen lassen, um diese Fähigkeiten noch weiter auszubauen. Daher kann man davon ausgehen, dass die Regierung den Versuch machen wird, diese Befugnisse weiter zu verankern und sie in künftigen Debatten über Gesetzreformen energisch zu verteidigen.

106. Es besteht auch ein erbärmlicher Mangel an kritischen Debatten über die Vorzüge und Nachteile des „besonderen Verhältnisses" des Vereinigten Königreichs zu den USA, seinen anderen „Five Eyes"-Partnern und den Ländern (einschließlich Deutschlands), die sich als Partner der „Five Eyes" an den unterschiedlichen Konfigurationen von „Five Eyes plus" beteiligt haben. Meiner Meinung nach stellt dies ein systematisches Versagen nationaler Debatten hinsichtlich der Auseinandersetzung mit der zentralen Aussage und den Implikationen von Snowdens Behauptung dar, dass Five Eyes als „supranationale Nachrichtenorganisation" zu verstehen ist, „die nicht den bekannten Gesetzen ihrer eigenen Länder entspricht". In Ermangelung einer derartigen Debatte besteht jede Möglichkeit, dass die gegenwärtigen transnationalen Vereinbarungen über den Nachrichtenaustausch größtenteils nicht von den bevorstehenden britischen Reformen betroffen sein werden.

---

[95] Chris Chambers, "The psychology of mass government surveillance: How do the public respond and is it changing our behaviour?", Guardian, 18. März 2015, verfügbar unter: http://www.ejiltalk.org/the-power-of- citizenship-bias/.

107. In diesem Zusammenhang und als Fazit kann man betonen, wie ich und andere an anderer Stelle kommentiert haben, dass, wenn nicht andere wichtige europäische Mächte die Messlatte in Bezug auf die Einschränkung der Überwachung und die demokratische Kontrolle ihrer eigenen Geheimdienste erheblich höher legen, insbesondere im Hinblick auf die Erfassung auslandsnachrichtendienstlicher Informationen, es einfach nicht glaubwürdig ist, dass andere dies vom Vereinigten Königreich erwarten.[96] Wie der britische Sonderbeauftragte für den Austausch von Informationen und Strafverfolgungsdaten kürzlich feststellte, ist der Aufbau eines neuen internationalen Rahmens für den grenzüberschreitenden Zugang zu Kommunikationsdaten in streng beschränkten und ordnungsgemäß überwachten Bedingungen die einzige greifbare Alternative zum internationalen Status Quo.

---

[96] Ilan Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, "Towards Multilateral Standards for Surveillance Reform", Oxford Internet Institute Discussion Paper, Januar 2015, verfügbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551164.