Sachverhalt

Die drei vorliegenden Beschwerden wurden nach den Enthüllungen von *Edward Snowden* betreffend die elektronischen Überwachungsprogramme der Geheimdienste der USA und des Vereinigten Königreichs erhoben. Die 16 Bf. halten es für wahrscheinlich, dass ihre elektronische Kommunikation aufgrund ihrer Aktivitäten (sie sind alle Journalisten oder Personen bzw. Organisationen, die sich für Bürgerrechte einsetzen) entweder (1) von den Geheimdiensten des Vereinigten Königreichs überwacht wurde, (2) von ausländischen Regierungen überwacht und dann von diesen Geheimdiensten erlangt wurde und/oder (3) durch die Behörden des Vereinigten Königreichs von Kommunikationsdienstleistern (»KDL«) erlangt wurde.

Edward Snowden hatte enthüllt, dass das *Government Communications Headquarter* (»GCHQ«, einer der Geheimdienste des Vereinigten Königreichs) eine Operation betrieb, mit der es Kommunikationsleitungen anzapfte und große Mengen von Daten speicherte. Ebenso kam heraus, dass das GCHQ geheimdienstliche Informationen über das *PRISM*- und das *Upstream*-Programm der amerikanischen NSA bezog. Über *PRISM* wurde geheimdienstliches Material von Internetserviceprovidern, über *Upstream* wurden Inhalte und Kommunikationsdaten von Glasfaserkabeln und Infrastrukturen der amerikanischen KDL gesammelt. Durch letztgenanntes Programm bestand ein weitreichender Zugang auch auf Daten von nichtamerikanischen Staatsbürgern.

Wesentlicher Bestandteil des nationalen Rechts über Massenüberwachungen ist das Gesetz über Ermittlungsbefugnisse (*Regulation of Investigatory Powers Act 2000*, im Folgenden: »RIPA«). Dessen § 8 Abs. 4 erlaubt es dem *Secretary of State*, Ermächtigungen für die »Überwachung ausländischer Kommunikation« zu erteilen. Maßnahmen nach dem RIPA konnten von Betroffenen vor dem unabhängigen Spezialgericht zur Kontrolle von Ermittlungsbefugnissen (*Investigatory Powers Tribunal*, im Folgenden: »IPT«) gerügt werden. Das RIPA sieht auch einen sogenannten Beauftragten für die Kommunikationsüberwachung (*Interception of Communications Commissioner*, im Folgenden: »ICC«) vor, der eine unabhängige Kontrolle der Wahrnehmung der Befugnisse und Pflichten unter diesem Gesetz zu gewährleisten hat. Der *Investigatory Powers Act* (»IPA«) 2016 ersetzte Teile des RIPA.

Der *Secretary of State* hat zudem von der im RIPA vorgesehenen Ermächtigung Gebrauch gemacht, die Befugnisse unter diesem Gesetz in einem Code of Practice (*Interception of Communication Code of Practice*, im Folgenden: »IC Code«) näher auszuführen.

Die Bf. des ersten und zweiten Falles gingen innerstaatlich nicht gerichtlich gegen die Verletzungen von Art. 8 EMRK vor, die durch die Überwachungsmaßnahmen angeblich bewirkt worden waren. Die zehn Bf. des dritten Falles erhoben diesbezüglich hingegen jeweils Beschwerden an das IPT, blieben damit aber weitgehend erfolglos.

Rechtsausführungen

Die Bf. rügten eine Verletzung von Art. 8 EMRK (hier: *Recht auf Achtung des Privatlebens*) durch drei verschiedene Regime, nämlich das Regime zur Massenüberwachung von Kommunikation nach § 8 Abs. 4 RIPA, das Regime zum Austausch geheimdienstlicher Informationen mit ausländischen Regierungen und das Regime zur Erlangung von Kommunikationsdaten unter Kapitel II RIPA. Ein Teil der Bf. rügte zudem eine Verletzung von Art. 10 EMRK (hier: *Pressefreiheit*), weil die Überwachungsregime keinen ausreichenden Schutz journalistischer Quellen oder vertraulichen journalistischen Materials vorsehen würden. Unter Art. 6 EMRK (*Recht auf ein faires Verfahren*) rügten die Bf. des dritten Falles überdies, dass die im IPT-Verfahren vorgesehenen Beschränkungen unverhältnismäßig gewesen seien und den Wesensgehalt des Rechts auf ein faires Verfahren beeinträchtigt hätten.

I. Nichterschöpfung des innerstaatlichen Instanzenzugs

(238) Die Regierung brachte vor, dass die Bf. des ersten und zweiten Falles den innerstaatlichen Instanzenzug nicht erschöpft hätten, da sie es verabsäumt hätten, ihre Rügen an das IPT heranzutragen. […]

(268) […] Der GH erkennt an, dass das IPT sich seit der Entscheidung im Fall *Kennedy/GB* im Jahr 2010 als ein wirksamer Rechtsweg erwiesen hat, den Bf., die sich über Handlungen der Geheimdienste und/oder den allgemeinen Betrieb von Überwachungsregimen beschweren, zunächst erschöpfen sollten, um den Anforderungen des Art. 35 Abs. 1 EMRK zu genügen. Er akzeptiert dennoch, dass den Bf. des ersten und zweiten Falles zur Zeit, als sie ihre Beschwerden erhoben, nicht vorgeworfen werden konnte, sich auf *Kennedy/GB* gestützt und behauptet zu haben, das IPT wäre kein wirksamer Rechtsbehelf für eine Rüge betreffend die allgemeine Konventionskonformität eines Überwachungsregimes. Er befindet daher, dass es spezielle Umstände gab, welche die Bf. von dem Erfordernis befreiten, ihre Rügen zuerst an das IPT heranzutragen, und dass ihre Beschwerden folglich nicht gemäß Art. 35 Abs. 1 EMRK für unzulässig erklärt werden können [, sondern für **zulässig** zu erklären sind] (mehrheitlich; *gemeinsames abweichendes Sondervotum der Richterin Pardalos und des Richters Eicke*).

II. Zur behaupteten Verletzung von Art. 8 EMRK

1. Das Regime nach § 8 Abs. 4 RIPA

(272) Der GH hält fest, dass diese Rüge nicht offensichtlich unbegründet […] und auch aus keinem anderen Grund unzulässig und deshalb für **zulässig** zu erklären ist (mehrheitlich im Hinblick auf die Bf. des ersten und zweiten Falles; einstimmig im Hinblick auf die Bf. des dritten Falles).

(307) In seiner Rechtsprechung zur Überwachung von Kommunikation im Strafverfahren entwickelte der GH die folgenden Mindestanforderungen, die gesetzlich festgelegt werden sollten, um einen Machtmissbrauch zu vermeiden: die Natur der Straftaten, die eine Überwachungsanordnung bewirken können; eine Definition der Personenkategorien, deren Kommunikation überwacht werden kann; eine Begrenzung der Dauer der Überwachung; das bei der Prüfung, Verwendung und Speicherung der erlangten Daten einzuhaltende Verfahren; die zu treffenden Vorkehrungen, wenn die Daten an andere mitgeteilt werden; und die Umstände, unter denen abgefangene Daten gelöscht oder zerstört werden können oder müssen. In *Roman Zakharov/RUS* bestätigte der GH, dass diese sechs Mindestanforderungen auch in Fällen gelten, wo die Überwachung aus Gründen der nationalen Sicherheit erfolgt. Bei der Entscheidung, ob die strittige Gesetzgebung gegen Art. 8 EMRK verstieß, berücksichtigte er allerdings auch die Vorkehrungen für die Kontrolle der Durchführung von Maßnahmen zur geheimen Überwachung, die Mechanismen zur Mitteilung und die vom nationalen Recht vorgesehenen Rechtsbehelfe.

(314) Der GH hat ausdrücklich anerkannt, dass die nationalen Behörden bei der Wahl, wie sie das legitime Ziel des Schutzes der nationalen Sicherheit am besten erreichen, einen weiten Ermessensspielraum genießen. Zudem hat er in *Weber und Saravia/D* und in *Liberty u.a./GB* akzeptiert, dass Regime zur Massenüberwachung nicht per se aus diesem Spielraum herausfallen. Obwohl beide Fälle mittlerweile mehr als zehn Jahre alt sind, befindet der GH angesichts seiner Begründung in diesen Urteilen und der gegenwärtigen Bedrohungen, denen sich viele Vertragsstaaten gegenübersehen (einschließlich der Geißel des globalen Terrorismus und anderer schwerwiegender Verbrechen wie Drogenhandel, Menschenhandel, die sexuelle Ausbeutung von Kindern und Cybercrime), technologischer Fortschritte, die es den Terroristen und Verbrechern leichter machen, der Entdeckung im Internet zu entkommen, und der Unvorhersehbarkeit der Wege, über die elektronische Kommunikation übermittelt wird, dass die Entscheidung, ein Regime zur Massenüberwachung in Betrieb zu nehmen, um bislang unbekannte Bedrohungen für die nationale Sicherheit zu identifizieren, weiterhin in den staatlichen Ermessensspielraum fällt.

(315) Dennoch ist es […] aus der Rechtsprechung des GH […] offenkundig, dass sowohl massenweise als auch gezielte Überwachungsregime potentiell missbraucht werden können, vor allem, wenn die wahre Weite des Ermessens der Behörden zur Überwachung aus der einschlägigen Gesetzgebung nicht erkennbar ist. Während die Staaten daher ein weites Ermessen dahingehend

genießen, welche Art von Überwachungsregime notwendig ist, um die nationale Sicherheit zu schützen, muss das ihnen beim Betrieb eines Überwachungsregimes gewährte Ermessen notwendigerweise enger sein. [...]

(320) [...] Demgemäß wird der GH die Rechtfertigung eines Eingriffs im vorliegenden Fall mit Bezugnahme auf die sechs Mindestanforderungen prüfen, die er falls notwendig adaptiert, damit sie den Betrieb eines Regimes zur Massenüberwachung widerspiegeln. Er wird auch die zusätzlichen relevanten Faktoren aus *Roman Zakharov/RUS* berücksichtigen, die er nicht als »Mindestanforderungen« klassifizierte [...] (siehe oben Rn.307).

a. Vorliegen eines Eingriffs

(321) Die Regierung bestreitet nicht, dass es einen Eingriff in die Rechte der Bf. nach Art. 8 EMRK gab.

b. Rechtfertigung des Eingriffs

(323) Die Parteien bestreiten nicht, dass das § 8 Abs. 4-Regime eine Grundlage im nationalen Recht hatte oder dass es die legitimen Ziele des Schutzes der nationalen Sicherheit, der Verhütung von Verbrechen und des Schutzes des wirtschaftlichen Wohles des Landes verfolgte. Die Bf. bestreiten hingegen die Qualität des innerstaatlichen Rechts und insbesondere seine [...] Vorhersehbarkeit.

i. Der Anwendungsbereich von geheimen Überwachungsmaßnahmen

(328) [...] In *Roman Zakharov/RUS* hat der GH klar gemacht, dass »das nationale Recht« laut [den beiden ersten der oben genannten Mindestanforderungen] »den Anwendungsbereich von Überwachungsmaßnahmen festlegen muss, indem es Bürgern einen angemessenen Hinweis auf die Umstände gibt, unter denen Behörden befugt sind, auf solche Maßnahmen zurückzugreifen«.

(329) [...] Im vorliegenden Fall [...] ist klar, dass sich das § 8 Abs. 4-Regime in vier verschiedene Stufen gliedert:

1. Die Überwachung eines geringen Prozentsatzes der Internetübertragungsleitungen, wobei diejenigen ausgewählt werden, die am wahrscheinlichsten ausländische[1] Kommunikationen von Interesse für den Geheimdienst transportieren;
2. das Filtern und automatische Ausscheiden (in beinahe Echtzeit) eines bedeutenden Prozentsatzes der abgefangenen Kommunikation [...];
3. die computergestützte Anwendung von einfachen und komplexen Suchkriterien auf die übrige Kommunikation, wobei jene, auf die die relevanten Selektoren zutreffen, behalten wird und die restliche ausgeschieden;
4. die Prüfung eines Teils oder des gesamten behaltenen Materials durch einen Analysten.

(330) [...] Der GH wird zuerst prüfen, ob die **Gründe**, aus denen eine Ermächtigung erteilt werden kann, **ausreichend klar** sind; zweitens, ob das innerstaatliche Recht den Bürgern einen angemessenen Hinweis auf die Umstände gibt, unter denen ihre Kommunikation überwacht werden kann; und drittens, ob das innerstaatliche Recht den Bürgern einen angemessenen Hinweis auf die Umstände gibt, unter denen ihre Kommunikation zur Prüfung ausgewählt werden kann.

(331) Gemäß dem RIPA und dem IC Code kann der *Secretary of State* eine Ermächtigung nur erteilen, wenn er davon überzeugt ist, dass sie im Interesse der **nationalen Sicherheit**, zur **Verhinderung oder Aufdeckung schwerwiegender Verbrechen** oder zum Schutz des wirtschaftlichen Wohles des Vereinigten Königreichs – sofern diese ebenfalls im Interesse der nationalen Sicherheit liegt – notwendig ist und dass das durch die Ermächtigung genehmigte Verhalten verhältnismäßig zum angestrebten Zweck ist. Laut dem innerstaatlichen Recht ist bei der Beurteilung der Notwendigkeit und Verhältnismäßigkeit zu berücksichtigen, ob die unter der Ermächtigung begehrten Informationen angemessen durch andere Mittel erlangt werden könnten (§ 5 Abs. 3 RIPA und Kapitel 6 des IC Codes). [...]

(333) In *Kennedy/GB* hatte der GH zu prüfen, ob die Gründe in § 5 Abs. 3 (die sowohl auf Ermächtigungen nach § 8 Abs. 1[2] als auch nach Abs. 4 Anwendung finden) ausreichend Details über die Natur der Straftaten boten, die eine Überwachungsanordnung zur Folge haben können. Er befand, dass der Begriff der »nationalen Sicherheit« in der nationalen und internationalen Gesetzgebung häufig verwendet wurde und eines der legitimen Ziele nach Art. 8 Abs. 2 EMRK darstellte. Er hielt auch fest, dass Bedrohungen der nationalen Sicherheit tendenziell im Charakter variieren und unvorhersehbar oder im Vorhinein schwer zu definieren sein können. Schließlich hatte der ICC bereits klargestellt, dass die »nationale Sicherheit« in der Praxis die Überwachung von Aktivitäten erlaubte, die die Sicherheit oder das Wohl des Staates bedrohten, sowie von Aktivitäten, die beabsichtigten, die parlamentarische Demokratie [...] zu untergraben oder zu stürzen. Der GH erachtete den Begriff daher für ausreichend klar.

(334) Zudem beobachtet der GH, dass der Begriff »schwerwiegende Verbrechen« in § 81 RIPA eindeutig definiert ist und dass der IC Code klargestellt hat, dass

1 Als ausländische Kommunikation gilt außerhalb der Britischen Inseln abgesendete oder empfangene Kommunikation.

2 § 8 Abs. 1 RIPA ermächtigt zur Ausstellung gezielter (das heißt auf bestimmte Personen oder Örtlichkeiten zugeschnittener) Überwachungsanordnungen.

der Zweck der Garantie des wirtschaftlichen Wohles des Vereinigten Königreichs auf die Interessen beschränkt ist, die auch für die nationale Sicherheit relevant sind.

(335) Der GH befindet daher, dass § 5 Abs. 3 [RIPA] ausreichend klar ist und den Bürgern angemessene Hinweise auf die Umstände bzw. Voraussetzungen gibt, unter denen eine Ermächtigung nach § 8 Abs. 4 [RIPA] erteilt werden kann.

(336) Was den **Kreis der Personen** betrifft, deren Kommunikation überwacht werden kann, ist klar, dass dieser weit ist. § 8 Abs. 4 erlaubt es dem *Secretary of State* nur, eine Ermächtigung für die Überwachung ausländischer Kommunikation zu erteilen. Das schließt Kommunikation grundsätzlich aus, bei der sich beide Parteien auf den Britischen Inseln befinden. […] Doch auch wenn klar ist, dass eine Kommunikation »inländisch« ist […], kann sie in der Praxis teilweise oder vollständig durch eines oder mehrere andere Länder geleitet werden und liefe daher Gefahr, unter dem § 8 Abs. 4-Regime abgefangen zu werden. Das wird von § 5 Abs. 6 RIPA ausdrücklich gestattet […].

(337) Abgesehen davon ist klar, dass die anvisierten Übertragungsleitungen nicht zufällig ausgewählt werden. Sie werden ausgewählt, weil angenommen wird, dass sie am wahrscheinlichsten ausländische Kommunikation von geheimdienstlichem Interesse beinhalten […]. Während unter dem § 8 Abs. 4-Regime potentiell die Kommunikation eines jeden überwacht werden konnte, ist daher klar, dass die Geheimdienste weder die Kommunikation aller überwachen noch ein uneingeschränktes Interesse genießen, jede Kommunikation zu überwachen, die sie überwachen möchten. In der Praxis muss einer der Gründe in § 5 Abs. 3 RIPA vorliegen, die Massenüberwachung muss verhältnismäßig zum angestrebten Ziel sein und es kann – zumindest auf der Makroebene der Auswahl der Übertragungsleitungen für die Überwachung – nur ausländische Kommunikation ins Visier genommen werden.

(338) […] Der GH hat bereits festgehalten, dass ein Regime zur Massenüberwachung den Behörden seiner Natur nach ein weites Ermessen zur Überwachung von Kommunikation einräumen wird und er befindet, dass dieser Umstand für sich alleine nicht in einem Widerspruch zu Art. 8 EMRK steht. Das Ermessen zur Überwachung darf zwar nicht unbeschränkt sein, da die Überwachung und Filterung von Kommunikation – auch wenn die Ausscheidung in der Folge beinahe in Echtzeit erfolgt – für einen Eingriff in die Rechte einer Person nach Art. 8 EMRK ausreicht. Allerdings werden für die dritte und vierte der oben in Rn. 329 identifizierten Stufen stärkere Garantien verlangt, nachdem ein Eingriff in solchen Fällen bedeutend größer sein wird.

(339) Was die **Auswahl von Kommunikation zur Überprüfung** nach dem Abfangen und Filtern angeht, wird jene, die nicht […] ausgeschieden wurde, weiter durchsucht. Zunächst geschieht dies durch die automatische Anwendung von einfachen Selektoren (wie Emailadresse oder Telefonnummer) und anfänglichen Suchkriterien […] und in der Folge durch die Verwendung einer komplexen Suche […].

(340) […] Im *Liberty*-Verfahren stellte das IPT fest, dass die Aufnahme der Selektoren in die Ermächtigung oder das Begleitzertifikat »die Durchführung der Ermächtigung unnötig untergraben und einschränken und jedenfalls völlig unrealistisch sein würde«. Der GH sieht keinen Grund, diese Schlussfolgerung in Frage zu stellen. Trotzdem sollten die zur Filterung abgefangener Kommunikation verwendeten Suchkriterien und Selektoren unabhängiger Kontrolle unterworfen sein – eine Garantie, die im § 8 Abs. 4-Regime zu fehlen scheint. […]

(341) Als Folge der Anwendung von Selektoren und automatischen Durchsuchungen wird ein Index erstellt. Nicht in den Index aufgenommenes Material wird ausgeschieden. Nur das in den Index aufgenommene Material darf **von einem Analysten geprüft** werden und nur, wenn es die zwei Kriterien in § 16 RIPA erfüllt, nämlich die Bescheinigung der Notwendigkeit durch den *Secretary of State* […] und die vorläufige Anwesenheit [des betroffenen Individuums] auf den Britischen Inseln […].

(342) Was die Bescheinigung […] angeht, beobachtete der Geheimdienst- und Sicherheitsausschuss des Parlaments (»GSA«), dass die Kategorien in diesen sehr allgemein angegeben wurden […] [und nicht mit Bezugnahme auf spezielle Operationen wie etwa konkrete Terroranschläge]. Der GH stimmt zu, dass es für die tatsächliche Wirksamkeit dieser Garantie höchst wünschenswert wäre, wenn die Bescheinigung spezifischer formuliert würde als dies aktuell der Fall zu sein scheint.

(343) Auf der anderen Seite stellt der Ausschluss der Kommunikation von Individuen, die sich aktuell bekanntermaßen auf den Britischen Inseln befinden, nach Ansicht des GH eine wichtige Garantie dar, da Personen, die für die Geheimdienste von Interesse sind und von denen bekannt ist, dass sie sich auf den Britischen Inseln aufhalten, einer gezielten Ermächtigung nach § 8 Abs. 1 RIPA unterworfen werden konnten. Den Geheimdiensten sollte es nicht gestattet sein, mit einer Massenermächtigung zu erhalten, was sie über eine gezielte Ermächtigung erhalten konnten.

(344) Gemäß § 7.18 des IC Codes mussten periodische Prüfungen erfolgen um sicherzustellen, dass die Anforderungen von § 16 RIPA erfüllt sind. Alle Verstöße gegen Garantien mussten dem ICC mitgeteilt werden. In seinem Jahresbericht 2016 […] hielt dieser fest, dass das Verfahren, mit dem Analysten Material für die Prüfung auswählten, das keine vorherige Genehmigung durch einen ranghöheren operativen Leiter erforderte, hauptsächlich auf das fachliche Urteil der Analysten […] gestützt war.

(345) Alles in allem wäre es für die Auswahl von Material durch Analysten zu bevorzugen, diese zumindest der vorherigen Genehmigung durch einen ranghöhe-

ren operativen Leiter zu unterwerfen. Da Analysten allerdings sorgfältig ausgebildet und geprüft sind, Aufzeichnungen geführt werden und diese Aufzeichnungen unabhängiger Kontrolle und Prüfung unterworfen sind, stellt das Fehlen einer vorherigen Genehmigung nicht bereits für sich ein Versäumnis dar, angemessene Garantien gegen Missbrauch zu gewähren.

(346) Dennoch muss der GH die Handhabung des § 8 Abs. 4-Regimes als Ganzes berücksichtigen und insbesondere den Umstand, dass die Liste, aus der die Analysten Material auswählen, selbst durch die Anwendung von Selektoren und Auswahlkriterien erstellt wird, die zuvor keiner unabhängigen Kontrolle unterworfen wurden. In der Praxis ist die einzige unabhängige Kontrolle des Verfahrens zur Filterung und Auswahl abgefangener Daten zur Prüfung die post factum-Überprüfung durch den ICC und das IPT, falls eine Beschwerde an dieses erhoben wird. […]

(347) Obwohl es keine Beweise dafür gibt, dass die Geheimdienste ihre Befugnisse missbrauchen – ganz im Gegenteil hielt der ICC fest, dass das Auswahlverfahren von den Analysten sorgfältig und gewissenhaft durchgeführt wurde –, ist der GH nicht überzeugt davon, dass die Garantien für die Auswahl der Übertragungsleitungen zur Überwachung und für die Auswahl von abgefangenem Material zur Prüfung ausreichend stark sind, um angemessen vor Missbrauch zu schützen. Zu den größten Bedenken veranlasst jedoch das Fehlen einer starken Kontrolle der zur Filterung der abgefangenen Kommunikation verwendeten Selektoren und Suchkriterien.

ii. Die Ausnahme dazugehöriger Kommunikationsdaten von den Garantien für die Durchsuchung und Prüfung des Inhalts

(348) Das Regime des Art. 8 Abs. 4 erlaubt die Massenüberwachung sowohl von Inhalten als auch von dazugehörigen Kommunikationsdaten (das »Wer, Wann und Wo« einer Kommunikation). § 16 findet hingegen nur auf »abgefangenes Material« Anwendung, das […] als Inhalt der abgefangenen Kommunikation definiert ist. Die abgefangenen dazugehörigen Kommunikationsdaten […] können daher ohne Beschränkungen durchsucht und für eine Prüfung ausgewählt werden.

(352) […] [Der GH] wird sich darauf konzentrieren, ob die von der Regierung gelieferte Erklärung, um dazugehörige Kommunikationsdaten von den Garantien [des § 16] auszunehmen (nämlich um die Wirksamkeit dieser Garantie im Hinblick auf Inhalte sicherzustellen)[3], zum verfolgten legitimen Ziel verhältnismäßig ist.

(353) Es unterliegt keinem Zweifel, dass Kommunikationsdaten eine wertvolle Quelle für Geheimdienste darstellen. Sie können rasch analysiert werden, um Muster herauszufinden, die besonderes Online-Verhalten im Zusammenhang mit Aktivitäten wie Terrorattacken widerspiegeln, und die Netzwerke und Verbindungen von in solche Attacken verwickelten Personen erhellen […]. Zudem sind sie anders als viele Inhaltsdaten nicht allgemein verschlüsselt.

(354) Außerdem akzeptiert der GH, dass die Wirksamkeit der Garantie des § 16 Abs. 2 [RIPA] davon abhängt, dass Geheimdienste ein Mittel besitzen um festzustellen, ob eine Person sich auf den Britischen Inseln befindet, und der Zugang zu dazugehörigen Kommunikationsdaten ihnen ein solches Mittel bietet.

(355) Trotzdem ist es in gewisser Weise besorgniserregend, dass die Geheimdienste »dazugehörige Kommunikationsdaten« offenkundig ohne Beschränkungen durchsuchen und prüfen können. Während solche Daten nicht mit der viel breiteren Kategorie der »Kommunikationsdaten« verwechselt werden dürfen, bilden sie dennoch eine bedeutende Datenmenge. Die Regierung versicherte […], dass unter § 8 Abs. 4 [RIPA] erlangte »dazugehörige Kommunikationsdaten« immer Verkehrsdaten sein werden. Gemäß den §§ 2.24-2.27 des *Code of Practice* über den Erwerb und die Offenlegung von Kommunikationsdaten (*Acquisition and Disclosure of Communications Data Code of Practice*, im Folgenden: »ACD Code«) schließen Verkehrsdaten allerdings solche Informationen ein, die den Ort des [für eine Kommunikation verwendeten] Geräts identifizieren […] (wie den Ort eines Mobiltelefons); die den Absender oder Empfänger […] einer Kommunikation aus Daten, die in der Kommunikation enthalten oder ihr beigefügt sind, identifizieren; Routing-Informationen, die Geräte identifizieren, über die eine Kommunikation übertragen wird oder wurde (z.B. zugewiesene dynamische IP-Adressen, Datenübertragungsprotokolle und Email-Header […]); Webbrowsing-Informationen, soweit nur ein Host-Rechner, Server, Domainname oder eine IP-Adresse offengelegt werden (anders gesagt sind Website-Adressen und […] »URLs« bis zum ersten Slash Kommunikationsdaten, nach dem ersten Slash aber Inhalte); […] und die Online-Verfolgung von Kommunikation […].

(356) Zudem ist der GH nicht überzeugt davon, dass der Erwerb von dazugehörigen Kommunikationsdaten notwendigerweise weniger eingriffsintensiv ist als der Erwerb von Inhalten. So kann der Inhalt einer elektronischen Kommunikation etwa verschlüsselt sein und selbst wenn er entschlüsselt werden sollte, nichts Bemerkenswertes über den Sender oder Empfänger enthüllen. Die dazugehörigen Kommunikationsdaten andererseits können die Identität und die geografische Lage des Senders und Empfängers […] offenlegen. In größeren Mengen wird das Ausmaß des Eingriffs verstärkt, da die auftauchenden Muster durch die Abbil-

3 Die Regierung brachte vor, dass der Zugang zu Kommunikationsdaten nötig sei um zu bestimmen, ob sich eine Person auf den Britischen Inseln befindet oder nicht.

dung sozialer Netzwerke, Standortortungen, die Nachverfolgung von Internetbrowsing, die Abbildung von Kommunikationsmustern und Einblicke dahingehend, mit wem eine Person interagierte, ein intimes Bild einer Person zeichnen können.

(357) Während der GH nicht daran zweifelt, dass dazugehörige Kommunikationsdaten für die Geheimdienste ein wesentliches Werkzeug im Kampf gegen den Terrorismus und schwere Verbrechen sind, befindet er daher nicht, dass die Behörden einen fairen Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen geschaffen haben, indem sie diese Daten vollständig von den Garantien ausnahmen, die auf die Durchsuchung und Prüfung von Inhalten angewendet werden. Der GH empfiehlt zwar nicht, dass dazugehörige Kommunikationsdaten nur dafür zugänglich sein sollen, um festzustellen, ob ein Individuum sich auf den Britischen Inseln befindet, da dies bedeuten würde, auf dazugehörige Kommunikationsdaten strengere Standards anzuwenden als auf Inhalte, doch müssen ausreichende Garantien eingerichtet sein um sicherzustellen, dass die Ausnahme von dazugehörigen Kommunikationsdaten von den Erfordernissen des § 16 RIPA auf das notwendige Ausmaß beschränkt wird um festzustellen, ob ein Individuum vorübergehend auf den Britischen Inseln weilt.

iii. Dauer der geheimen Überwachungsmaßnahme

(358) Gemäß § 9 RIPA verlor eine Ermächtigung nach § 8 Abs. 4 ihre Wirkung am Ende des »betreffenden Zeitraums«, wenn sie nicht erneuert wurde. Für Ermächtigungen, die vom *Secretary of State* aus Gründen der nationalen oder wirtschaftlichen Sicherheit gewährt wurden, beträgt der »betreffende Zeitraum« sechs Monate, und bei solchen, die vom *Secretary of State* aus Gründen der Verhütung schwerwiegender Verbrechen gewährt wurden, drei Monate. Diese Ermächtigungen können jeweils für Zeitspannen von sechs bzw. drei Monaten verlängert werden. Ermächtigungen können zu jedem Zeitpunkt vor ihrem Ablaufdatum durch Antrag an den *Secretary of State* erneuert werden. Der Antrag muss dieselben Informationen wie der ursprüngliche Antrag und auch eine Einschätzung des Nutzens der bisherigen Überwachung enthalten und erklären, warum deren Fortsetzung notwendig […] und verhältnismäßig ist. § 6.7 des IC-Codes verlangt die regelmäßige Überprüfung entsprechender Kommunikationsverbindungen. […]

(359) Zudem muss der *Secretary of State* eine Ermächtigung widerrufen, wenn er überzeugt davon ist, dass sie […] nicht länger notwendig ist […].

(360) Im Fall *Kennedy/GB* prüfte der GH dieselben Bestimmungen über die Dauer und Erneuerung von Ermächtigungen zur Überwachung […] und befand, dass die Regelungen ausreichend klar waren, um angemessene Garantien gegen Missbrauch zu gewähren. Insbesondere hielt er fest, dass die Pflicht des *Secretary of State*, Ermächtigungen aufzuheben, die nicht länger notwendig waren, praktisch bedeutete, dass die Geheimdienste ihre Ermächtigungen einer fortdauernden Überprüfung unterziehen mussten. Im Lichte der vorangehenden Erwägungen sieht der GH keine Gründe, aus denen er im vorliegenden Fall zu einem anderen Schluss kommen könnte. […]

iv. Zum einzuhaltenden Verfahren

(361) […] Analysten können nur Material untersuchen, das auf dem automatisch generierten Index erscheint. Bevor sie Material auf dem Index lesen, ansehen oder anhören können, müssen sie aufzeichnen, warum der Zugang zu dem Material für einen der in § 5 Abs. 3 RIPA vorgesehenen Zwecke notwendig und […] verhältnismäßig ist […]. Gemäß § 16 Abs. 2 können sie kein Material zur Prüfung auswählen, indem sie Kriterien verwenden, die sich auf die Kommunikation von Individuen beziehen, von denen bekannt ist, dass sie sich aktuell auf den Britischen Inseln aufhalten. § 7.16 des IC Codes verlangt vom Analysten auch, Umstände anzugeben, die wahrscheinlich eine gewisse begleitende Verletzung der Privatsphäre bewirken, zusammen mit den Maßnahmen, die gesetzt wurden, um das Ausmaß des Eingriffs zu reduzieren. Der folgende Zugriff des Analysten ist auf eine festgelegte Zeitspanne begrenzt. Diese Periode kann zwar verlängert werden, doch müssen die Aufzeichnungen auf den neuesten Stand gebracht und Gründe für die Verlängerung angeführt werden.

(362) § 7.15 verlangt ferner, dass Analysten, die abgefangenes Material untersuchen, dazu speziell autorisiert sein müssen, regelmäßiges verpflichtendes Training im Hinblick auf die Bestimmungen des RIPA und speziell die Umsetzung von § 16 sowie die Erfordernisse der Notwendigkeit und Verhältnismäßigkeit erhalten und kontrolliert werden müssen. Zudem werden regelmäßige Prüfungen durchgeführt, die Kontrollen einschließen müssen um sicherzustellen, dass die Aufzeichnungen im Zusammenhang mit dem Zugang zu Material korrekt erstellt wurden und dass das verlangte Material unter die Angelegenheiten fällt, die der *Secretary of State* bescheinigt hat […].

(363) Was die Speicherung von abgefangenem Material anbelangt, verlangt § 7.7 des IC Codes, dass es vor seiner Vernichtung sicher gelagert werden muss und keiner Person zugänglich sein darf, die nicht die erforderliche Sicherheitsfreigabe hat.

(364) Angesichts des Vorgesagten und seiner Schlussfolgerungen in den Rn. 347 und 357 oben akzeptiert der GH, dass die Bestimmungen betreffend die Speicherung abgefangener Daten, den Zugang zu ihnen sowie ihre Prüfung und Verwendung ausreichend klar sind.

v. Mitteilung der abgefangenen Daten an andere

(365) Während das Material gespeichert ist, verlangen § 15 Abs. 2 RIPA und § 7.2 des IC Codes, dass Folgendes auf das für die erlaubten Zwecke notwendige Minimum beschränkt wird: Die Zahl der Personen, denen das Material oder Daten offengelegt oder verfügbar gemacht werden; das Ausmaß, in dem das Material oder Daten offengelegt oder verfügbar gemacht werden; das Ausmaß, in dem das Material oder Daten kopiert werden; und die Zahl der gemachten Kopien. Gemäß § 15 Abs. 4 und § 7.2 des IC Codes ist etwas für die erlaubten Zwecke nur notwendig, wenn es weiterhin notwendig ist oder wahrscheinlich notwendig werden wird für die in § 5 Abs. 3 RIPA erwähnten Ziele; für die Erleichterung der Durchführung einer der Überwachungsfunktionen des *Secretary of State*; zur Erleichterung der Durchführung von Funktionen des ICC oder des IPT; für die Sicherstellung, dass jemand, der eine Strafverfolgung durchführt, die Informationen hat, die er benötigt […], um die Fairness des Verfahrens zu garantieren […].

(366) § 7.3 des IC Codes verbietet die Offenlegung gegenüber Personen, die nicht angemessen überprüft wurden und auch durch den *need-to-know*-Grundsatz: Abgefangenes Material darf niemandem offengelegt werden, außer die Aufgaben desjenigen, die in Verbindung mit einem der genehmigten Zwecke stehen müssen, verlangen für ihre Wahrnehmung, dass dieser Kenntnis von dem abgefangenen Material hat. Gleichfalls darf nur so viel von dem abgefangenen Material offengelegt werden, wie der Empfänger braucht. § 7.3 findet gleichermaßen auf die Offenlegung gegenüber weiteren Personen innerhalb der Behörde und die Offenlegung außerhalb der Behörde Anwendung. Gemäß § 7.4 ist er nicht nur auf das ursprünglich überwachende Organ anzuwenden, sondern auch auf jeden, dem das abgefangene Material später offengelegt wird.

(367) Wenn abgefangenes Material Behörden eines Landes oder Hoheitsgebietes außerhalb des Vereinigten Königreichs offengelegt wird, muss die Behörde gemäß § 7.5 des IC Codes angemessene Schritte setzen um sicherzustellen, dass die fraglichen Behörden die nötigen Verfahren haben und beibehalten, um das abgefangene Material zu schützen, und dass es nur in dem nötigen Mindestumfang offengelegt, kopiert, weitergegeben und gespeichert wird. Es darf nicht Behörden eines dritten Landes oder Hoheitsgebietes offengelegt werden, außer dies wurde mit der herausgebenden Behörde ausdrücklich vereinbart. Es muss zudem an die herausgebende Behörde zurückgegeben oder sicher vernichtet werden, wenn es nicht länger gebraucht wird.

(368) […] Da »wahrscheinlich notwendig werden« im RIPA oder IC Code oder woanders nicht genauer definiert wird, konnte den Behörden dadurch in der Praxis eine weitgreifende Befugnis eingeräumt werden, abgefangenes Material offenzulegen und zu kopieren. Dennoch ist klar, dass auch wenn eine Offenlegung oder Kopie für einen »erlaubten Zweck« »wahrscheinlich notwendig wird«, das Material trotzdem nur einer Person offengelegt werden kann, die über die angemessene Sicherheitsfreigabe verfügt und ein Interesse nach dem *need-to-know*-Grundsatz hat. Zudem ist nur so viel des abgefangenen Materials offenzulegen, wie das Individuum wissen muss […].

(369) Während es daher wünschenswert wäre, dass der Begriff »wahrscheinlich notwendig werden« entweder im RIPA oder IC Code genauer definiert wird, befindet der GH dennoch, dass § 15 RIPA und Kapitel 7 des IC Code insgesamt gesehen angemessene Garantien für den Schutz der erlangten Daten gewähren.

vi. Die Umstände, unter denen abgefangenes Material gelöscht oder vernichtet werden muss

(370) § 15 Abs. 3 RIPA und § 7.8 des IC Code verlangen, dass jede Kopie von abgefangenem Material oder abgefangenen Daten […] verlässlich gelöscht wird, sobald die Speicherung nicht länger für einen der Zwecke in § 5 Abs. 3 notwendig ist. In der Praxis bedeutet das, dass abgefangenes Material, das beinahe in Echtzeit herausgefiltert wird, zerstört wird. Ähnlich wird nach der Anwendung von Selektoren und Suchkriterien Material vernichtet, das nicht dem Index des Analysten hinzugefügt wird.

(371) § 7.9 sieht vor, dass ein Geheimdienst, der nicht analysiertes abgefangenes Material und dazugehörige Kommunikationsdaten über eine Überwachung nach einer Ermächtigung unter § 8 Abs. 4 erhält, Maximalspeicherperioden für verschiedene Datenkategorien festlegen muss, die ihre Natur und den Umfang ihres Eingriffs widerspiegeln. Diese Perioden sollten normalerweise nicht länger als zwei Jahre sein und mit dem ICC abgestimmt werden. Soweit möglich, sollten alle Speicherzeiträume durch einen Prozess automatischer Löschung realisiert werden, der ausgelöst wird, sobald die anwendbare Maximalspeicherdauer für das fragliche Datum erreicht wird. Gemäß § 7.8 ist abgefangenes Material, das behalten wird, in angemessenen Intervallen zu überprüfen, um sich zu vergewissern, dass die Rechtfertigung für seine Speicherung immer noch iSd. § 15 Abs. 3 RIPA gültig ist.

(372) Gemäß dem Jahresbericht 2016 des ICC hatte jede Überwachungsbehörde eine andere Sichtweise, was eine angemessene Speicherdauer für abgefangenes Material und dazugehörige Kommunikationsdaten darstellte. Die Speicherdauer für Inhalte reichte von dreißig Tagen bis zu einem Jahr und jene für dazugehörige Kommunikationsdaten von sechs Monaten bis zu einem Jahr. […] Es ist daher klar, dass [die festgelegten Speicherzeiträume] zwei Jahre nicht übersteigen können und in der Praxis ein Jahr nicht übersteigen […].

(373) Zudem kann das IPT, wenn an dieses eine Beschwerde erhoben wird, prüfen, ob die Speicherfristen eingehalten wurden, und – wenn dies nicht der Fall

ist – feststellen, dass eine Verletzung von Art. 8 EMRK erfolgt ist, und die Vernichtung des betreffenden Materials anordnen. Wenn die Speicherung zu einem Schaden oder Nachteil geführt hat, kann auch eine Entschädigung zugesprochen werden. […]

(374) Deshalb sind nach Ansicht des GH die Bestimmungen über die Löschung und Vernichtung von abgefangenem Material ebenfalls ausreichend klar.

vii. Kontrolle, Mitteilung und Rechtsbehelfe

(375) Eine Kontrolle des Regimes erfolgt auf einer Reihe von Ebenen. Erstens wird gemäß dem ICC »vom Personal und von den Juristen **innerhalb der überwachenden Behörde** oder der die Ermächtigungen erteilenden Abteilung anfangs eine kritische qualitätssichernde Funktion wahrgenommen«. Die Ermächtigungen gewährenden Abteilungen bieten dem *Secretary of State* eine unabhängige Beratung und führen eine wichtige Überprüfung von Anträgen auf Ermächtigungen und Erneuerungen vor deren Genehmigung durch um sicherzustellen, dass sie notwendig und verhältnismäßig sind und bleiben.

(376) Zweitens müssen Ermächtigungen nach § 8 Abs. 4 durch den ***Secretary of State*** genehmigt werden. […] Während der GH anerkannt hat, dass eine gerichtliche Genehmigung eine »wichtige Garantie gegen Willkür« ist, hat er diese bislang nicht als »notwendiges Erfordernis« angesehen. Obwohl sie grundsätzlich wünschenswert ist, ist sie für sich weder notwendig noch ausreichend, um eine Beachtung von Art. 8 EMRK sicherzustellen.

(378) Im vorliegenden Fall gibt es keinen Beweis dafür, dass der *Secretary of State* Ermächtigungen ohne gebührende Überprüfung erteilt. Das Genehmigungsverfahren war einer unabhängigen Kontrolle durch den ICC […] unterworfen. Dieser war von der Exekutive und Legislative unabhängig, hatte ein hohes richterliches Amt inne oder innegehabt und war mit der Aufgabe betraut, die allgemeine Funktion des Überwachungsregimes sowie die Erteilung von Überwachungsermächtigungen in speziellen Fällen zu beaufsichtigen. Der *Commissioner* berichtete jährlich an den Premierminister. Sein Bericht war ein öffentliches Dokument […], das dem Parlament vorgelegt wurde. Bei der Wahrnehmung seiner Überprüfung von Überwachungspraktiken wurde ihm Zugang zu allen relevanten Dokumenten gewährt […]. Die Verpflichtung der Geheimdienste, Aufzeichnungen zu führen, stellte sicher, dass er wirksamen Zugang zu den Details der vorgenommenen Überwachungsaktivitäten hatte. […] Als Folge akzeptierte der GH in *Kennedy/GB*, dass trotz des Umstands, dass die Ermächtigung nach § 8 Abs. 1 durch den *Secretary of State* erteilt wurde, durch den ICC eine ausreichende Unabhängigkeit gewährt wurde.

(379) Zudem hat das **IPT** umfassende Jurisdiktionsbefugnis, um jede Beschwerde wegen unrechtmäßiger Überwachung zu untersuchen: Anders als in vielen anderen Staaten hängt seine Jurisdiktion nicht von der Mitteilung der Überwachung an das Subjekt ab, was bedeutet, dass jede Person, die glaubt, geheimer Überwachung unterworfen worden zu sein, sich bei ihm beschweren kann. Seine Mitglieder müssen ein hohes richterliches Amt innehaben oder innegehabt haben oder qualifizierte Anwälte […] sein. Die an der Genehmigung und Durchführung einer Überwachungsermächtigung Beteiligten sind verpflichtet, ihm alle Dokumente offenzulegen, die es verlangt – auch […] Dokumente, die aus Gründen der nationalen Sicherheit nicht öffentlich gemacht werden konnten. Es hat Ermessen, mündliche und wenn möglich öffentliche Verhandlungen abzuhalten. In nicht öffentlichen Verfahren kann es den *Counsel to the Tribunal*[4] dazu bevollmächtigen, auch Eingaben im Namen von Bf. zu tätigen, die nicht vertreten werden können. Wenn es über eine Beschwerde entscheidet, hat es die Befugnis, eine Entschädigung zuzusprechen und jede andere Anordnung zu treffen, die es für angebracht erachtet, einschließlich der Aufhebung oder Annullierung einer Ermächtigung und des Verlangens, Aufzeichnungen zu vernichten. Die Veröffentlichung der […] Entscheidungen des IPT verstärkt das Maß an Überprüfung weiter […].

(381) Während der GH eine gerichtliche Genehmigung für höchst wünschenswert erachtet […], akzeptiert er im vorliegenden Fall [insbesondere] angesichts der Überprüfung von Anträgen auf Ermächtigungen vor der Genehmigung, der umfassenden Überprüfung nach der Genehmigung durch das (unabhängige) Büro des *Commissioners* und das IPT […], dass die Genehmigung von Ermächtigungen nach § 8 Abs. 4 durch den *Secretary of State* für sich keine Verletzung von Art. 8 EMRK bewirkt.

(382) Schließlich erinnert der GH daran, dass vor dem Hintergrund der Enthüllungen durch *Edward Snowden* gründliche unabhängige Überprüfungen der bestehenden Überwachungsregime erfolgten und keines der Überprüfungsorgane einen Beweis dafür entdeckte, dass ein bewusster Missbrauch von Überwachungsbefugnissen stattfand.

(383) Im Lichte der vorangehenden Erwägungen ist der GH der Ansicht, dass die Kontrolle der Massenüberwachungen geeignet ist, angemessene und wirksame Garantien gegen Missbrauch zu gewähren.

viii. Verhältnismäßigkeit

(384) […] Der GH bemerkt, dass der *Independent Reviewer of Terrorism Legislation*[5] eine große Menge an gesperrtem Material überprüfte und zum Schluss kam, dass der Massenüberwachung ein wesentliches Potential innewohnte. Obwohl er […] nach Alternativen zur Massen-

4 Dieser kann vom IPT in Fällen bestellt werden, in denen die Interessen bestimmter Parteien nicht wahrgenommen werden können, damit er aus deren Perspektive Eingaben tätigt.

5 Die Aufgabe dieser unabhängigen Person ist es, an den Innenminister und das Parlament über die Durchführung von Antiterrorgesetzen im Vereinigten Königreich zu berichten.

überwachung Ausschau hielt [...], kam er zum Schluss, dass die Stärke der Massenüberwachung durch keine Alternative oder Kombination von Alternativen ersetzt werden konnte.

(385) Ähnlich [...] anerkannte die Venedig-Kommission den immanenten Wert [der Massenüberwachung] für Sicherheitsoperationen [...].

(386) Der GH sieht keinen Grund, um der gründlichen Prüfung durch diese beiden Organe und den von ihnen erreichten Schlussfolgerungen nicht zuzustimmen. Es ist klar, dass Massenüberwachung ein wertvolles Mittel ist, um die verfolgten legitimen Ziele zu erreichen [...].

c. Ergebnis

(387) Im Lichte der vorangegangenen Erwägungen befindet der GH, dass die Entscheidung, ein Regime zur Massenüberwachung zu betreiben, in den weiten Ermessensspielraum des Vertragsstaates fiel. Zudem ist er [...] überzeugt davon, dass die Geheimdienste des Vereinigten Königreichs ihre Konventionsverpflichtungen ernst nehmen und ihre Befugnisse unter § 8 Abs. 4 RIPA nicht missbrauchen. Dennoch hat eine Prüfung dieser Befugnisse [folgende] Bedenken [...] hervorgerufen: Erstens das Fehlen von Kontrolle für den gesamten Auswahlprozess, einschließlich der Auswahl von Übertragungsleitungen für die Überwachung, der Selektoren und Suchkriterien zur Filterung abgefangener Kommunikation und der Auswahl von Material zur Prüfung durch einen Analysten, und zweitens das Fehlen von wirklichen Garantien, die auf die Auswahl von dazugehörigen Kommunikationsdaten zur Prüfung Anwendung finden.

(388) Angesichts dieser Mängel und im soeben dargelegten Ausmaß befindet der GH, dass das § 8 Abs. 4-Regime die Anforderungen an die »Qualität des Gesetzes« nicht erfüllt und den »Eingriff« nicht auf das beschränken kann, was »in einer demokratischen Gesellschaft notwendig« ist. Es erfolgte daher eine **Verletzung** von **Art. 8 EMRK** (5:2 Stimmen; *gemeinsames abweichendes Sondervotum der Richterin Pardalos und des Richters Eicke; im Ergebnis übereinstimmendes Sondervotum von Richter Koskelo, gefolgt von Richter Turković*).

2. Das Regime zum Informationsaustausch

(389) Die Bf. des dritten Falles rügen, dass der Erhalt von durch die NSA unter *PRISM* und *Upstream* abgefangenem Material durch den belangten Staat ihre Rechte unter Art. 8 EMRK verletzte. Die Bf. des ersten Falles beschweren sich mehr allgemein über den Erhalt von Informationen von ausländischen Geheimdiensten.

(396) [...] Der GH akzeptiert, dass die Bf. potentiell Gefahr liefen, dass ihre Kommunikation durch die Geheimdienste des belangten Staates unter dem Regime zum Informationsaustausch erlangt wurden. Daher können sie behaupten, [...] Opfer der behaupteten Verletzung aufgrund dieses Regimes zu sein.

(397) Diese Rüge ist nicht offensichtlich unbegründet [...] und auch aus keinem anderen Grund unzulässig und deshalb für **zulässig** zu erklären (einstimmig).

a. Umfang der Rügen der Bf.

(416) Dies ist das erste Mal, dass der GH ersucht wurde, die Konventionskonformität eines Regimes zum Informationsaustausch zu prüfen. Während der Betrieb eines solchen Systems eine Reihe von Fragen unter der Konvention aufwerfen kann, konzentrieren sich die Rügen der Bf. betreffend das Regime, mit dem die Behörden des Vereinigten Königreichs ausländische Regierungen um Geheimdienstinformationen ersuchen und diese erhalten, im vorliegenden Fall auf Art. 8 EMRK. Die Bf. rügen nicht die Weitergabe von solchen Informationen durch die Geheimdienste des Vereinigten Königreichs an ausländische Gegenüber und berufen sich auch nicht auf andere Konventionsbestimmungen.

(417) [...] Der GH wird seine Prüfung auf jenes Material beschränken, das [...] Kommunikation betrifft, welche die Geheimdienste des Vereinigten Königreichs die NSA gebeten haben abzufangen oder ihnen – soweit bereits abgefangen – zur Verfügung zu stellen.

b. Die Natur des Eingriffs

(420) Obwohl das strittige Regime abgefangene Kommunikation betrifft, liegt der zu berücksichtigende Eingriff in diesem Fall nicht in der Überwachung selbst, die jedenfalls nicht unter der Hoheitsgewalt des Vereinigten Königreichs erfolgte und diesem nach Völkerrecht nicht zugerechnet werden konnte. [...]

(421) Der Eingriff liegt in der Annahme des abgefangenen Materials und der folgenden Speicherung, Prüfung und Verwendung durch dessen Geheimdienste.

c. Der anwendbare Test

(423) Die Parteien sind sich nicht einig dahingehend, ob die sechs Mindestanforderungen [siehe oben Rn. 307], die gemeinhin in Fällen betreffend die Überwachung von Kommunikation Anwendung finden [...], im vorliegenden Fall ebenfalls anwendbar sein sollen. Es trifft zu, dass der Eingriff in diesem Fall nicht durch die Überwachung von Kommunikation durch den belangten Staat erfolgte. Da das erlangte Material aber Produkt von Überwachungen ist, müssen die Voraussetzungen, die sich auf seine Speicherung, Prüfung, Verwendung, weitere Verbreitung, Löschung und Vernichtung beziehen, gegeben sein. [...]

(424) [...] Der GH bedenkt [...], dass dann, wenn die Vertragsstaaten ein unbegrenztes Ermessen genießen würden, um entweder die Überwachung von Kommu-

nikation oder die Übermittlung von abgefangener Kommunikation durch Nichtvertragsstaaten zu verlangen, sie ihre Verpflichtungen unter der Konvention leicht umgehen könnten. Folglich müssen die Umstände, unter denen abgefangenes Material von ausländischen Geheimdiensten verlangt werden kann, auch im innerstaatlichen Recht festgelegt sein, um den Missbrauch von Macht zu vermeiden. Während die Umstände, unter denen ein solches Ersuchen ergehen kann, nicht mit den Umständen identisch sein mögen, unter denen ein Staat selbst solche Maßnahmen vornimmt [...], müssen sie doch ausreichend umschrieben sein, um Staaten soweit wie möglich davon abzuhalten, diese Befugnis zu verwenden, um entweder das innerstaatliche Recht oder ihre Konventionsverpflichtungen zu umgehen.

d. Anwendung des Tests auf das fragliche Material

i. Zugänglichkeit

(425) Der gesetzliche Rahmen, der es den Geheimdiensten des Vereinigten Königreichs erlaubt, abgefangenes Material von ausländischen Geheimdiensten zu verlangen, ist nicht im RIPA enthalten. Das britisch-amerikanische *Communication Intelligence Agreement* vom 5.3.1946[6] erlaubt speziell den Austausch von Material zwischen den Vereinigten Staaten und dem Vereinigten Königreich. Allgemeiner legen das Gesetz über die Sicherheitsdienste (*Security Services Act*, »SSA«) und das Gesetz über die Geheimdienste (*Intelligence Services Act*, »ISA«) die Funktion der Geheimdienste dar und verlangen, dass Regelungen getroffen werden um sicherzustellen, dass von ihnen nur Informationen erlangt werden, die für die ordentliche Erfüllung ihrer Aufgaben notwendig sind; und dass von ihnen keine Informationen offengelegt werden, außer soweit dies zu diesem Zweck oder für den Zweck von Strafverfahren notwendig ist.

(426) Details der internen Regelungen, auf die im SSA und ISA Bezug genommen wird [...], wurden nun in den jüngsten IC Code aufgenommen.

(427) Folglich befindet der GH, dass es nun eine rechtliche Grundlage für das Ersuchen um Geheimdienstinformationen von ausländischen Geheimdiensten gibt und dass dieses Recht ausreichend zugänglich ist. Zudem verfolgt dieses Regime eindeutig mehrere legitime Ziele, einschließlich der nationalen und öffentlichen Sicherheit, des wirtschaftlichen Wohles des Landes, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer. Es obliegt dem GH daher, die Vorhersehbarkeit und Notwendigkeit des Regimes zu beurteilen. [...]

ii. Die Umstände, unter denen abgefangenes Material verlangt werden kann

(428) Kapitel 12 des IC Codes hält fest, dass die Geheimdienste außer unter außergewöhnlichen Umständen lediglich dann ein Ersuchen an eine ausländische Regierung im Hinblick auf nicht ausgewertete abgefangene Kommunikation und/oder dazugehörige Kommunikationsdaten stellen dürfen, wenn vom *Secretary of State* bereits eine Ermächtigung zur Überwachung unter dem RIPA erteilt wurde, die Unterstützung der ausländischen Regierung notwendig ist, um die besondere Kommunikation zu erlangen, weil sie nicht unter der bestehenden Ermächtigung erlangt werden kann, und es für die überwachende Behörde notwendig und verhältnismäßig ist, diese Kommunikationen zu erlangen. [...]

(429) Wenn außergewöhnliche Umstände vorliegen, kann ein Ersuchen um Kommunikation ohne eine einschlägige Ermächtigung nach dem RIPA nur dann gestellt werden, wenn es keine bewusste Umgehung des RIPA darstellt oder dessen Ziele auf andere Weise vereitelt [...] und es für die überwachende Behörde notwendig und verhältnismäßig ist, diese Kommunikationen zu erlangen. In einem solchen Fall muss das Ersuchen vom *Secretary of State* persönlich geprüft und von diesem darüber entschieden werden. Gemäß dem geänderten IC Code muss es auch dem ICC mitgeteilt werden. [...]

(430) Angesichts der obigen Erwägungen befindet der GH, dass die Umstände, unter denen der belangte Staat eine Überwachung oder die Übermittlung von abgefangenem Material verlangen kann, im innerstaatlichen Recht ausreichend umschrieben sind, um den Staat davon abzuhalten, diese Befugnis dazu zu verwenden, entweder das innerstaatliche Recht oder seine Konventionsverpflichtungen zu umgehen.

iii. Das einzuhaltende Verfahren

(431) Gemäß § 19 Abs. 2 des Antiterror-Gesetzes (*Counter-Terrorism Act*, »CTA«) 2008 dürfen Informationen, die von Geheimdiensten in Verbindung mit der Ausübung ihrer Funktionen erlangt werden, in Verbindung mit der Ausübung ihrer anderen Funktionen verwendet werden. Die Geheimdienste sind jedoch verpflichtet, die Datenschutzgrundsätze nach Teil 1 Anhang 1 zum Datenschutzgesetz (*Data Protection Act*) einzuhalten. [...] Sie können keine Ausnahmen von der Verpflichtung erhalten, [...] persönliche Daten, die für einen bestimmten Zweck verarbeitet werden, nicht länger aufzubewahren als für diesen Zweck nötig ist. Zudem sind angemessene technische und organisatorische Maßnahmen gegen die nicht genehmigte oder unrechtmäßige Verarbeitung von persönlichen Daten und gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Vernichtung oder Beschädigung von persönlichen Daten zu setzen. [...]

6 Dieses Abkommen beinhaltet Regelungen zum Austausch von Geheimdienstinformationen im Zusammenhang mit Kommunikation aus Drittstaaten.

(432) [...] Die Garantien in den §§ 15 und 16 RIPA in ihrer Ergänzung durch Kapitel 7 des IC Codes finden gleichermaßen auf abgefangene Kommunikationen und Kommunikationsdaten Anwendung, die von ausländischen Regierungen erlangt wurden.

(433) Der GH hat die Garantien in den §§ 15 und 16 RIPA in ihrer Ergänzung durch Kapitel 7 des IC Codes bereits sorgfältig geprüft, als er das § 8 Abs. 4-Regime beurteilt hat (siehe oben Rn. 361-363). [...]

(435) Im Lichte des Vorgesagten akzeptiert der GH, dass die Bestimmungen betreffend die Speicherung solchen Materials, den Zugang zu ihm sowie seine Prüfung und Verwendung ausreichend klar sind.

iv. Mitteilung des erlangten Materials an andere Parteien

(436) Wie bei Material, das direkt aufgrund einer Ermächtigung unter dem RIPA abgefangen wird (siehe oben Rn. 365-367), muss die Offenlegung von Material, das von ausländischen Geheimdiensten erlangt wurde, auf das Minimum beschränkt werden, das für die in § 5 Abs. 3 RIPA erwähnten erlaubten Zwecke notwendig ist. Zusätzlich ist die Offenlegung gegenüber Personen verboten, die nicht angemessen überprüft wurden, und Material darf nur gegenüber einer Person offengelegt werden, deren Aufgaben in Bezug zu einem der erlaubten Zwecke stehen und es notwendig machen, dass sie Kenntnis von diesem Material hat [...].

(437) § 19 Abs. 3-5 des CTA sehen weiters vor, dass vom MI5 oder MI6 im Hinblick auf ihre Funktionen erlangte Informationen von ihnen zum Zweck der ordnungsgemäßen Wahrnehmung ihrer Funktionen offengelegt werden dürfen; im Interesse der nationalen Sicherheit, zum Zweck der Verhinderung oder Aufdeckung von schwerwiegenden Verbrechen; oder für den Zweck eines Strafverfahrens. Vom GCHQ erhaltene Informationen dürfen von diesem zum Zweck der ordnungsgemäßen Wahrnehmung seiner Funktionen oder für den Zweck eines Strafverfahrens offengelegt werden.

(439) Angesichts des Vorgesagten akzeptiert der GH ebenfalls, dass die Bestimmungen betreffend das Verfahren, das für die Kommunikation des erlangten Materials an andere Parteien zu verfolgen ist, ausreichend klar sind.

v. Die Umstände, unter denen das erlangte Material gelöscht oder vernichtet werden muss

(440) § 15 Abs. 3 RIPA und § 7.8 des IC Codes verlangen, dass jede Kopie [...] sicher vernichtet werden muss, sobald die Speicherung für die Zwecke des § 5 Abs. 3 nicht länger notwendig ist.

vi. Überwachung und Rechtsmittel

(441) In beinahe jedem Fall wird eine Ermächtigung nach § 8 Abs. 1 oder Abs. 4 vorliegen, was bedeutet, dass der *Secretary of State* (und nach Inkrafttreten des IPA 2016 ein richterlicher Beauftragter) die Überwachung bereits genehmigt hat. Unter außergewöhnlichen Umständen – wenn keine Ermächtigung besteht – muss der *Secretary of State* das Ersuchen persönlich prüfen und darüber entscheiden und der ICC (nun der *Investigatory Power Commissioner*) muss benachrichtigt werden. Daher wird der *Secretary of State* in jedem Fall, in dem ein Ersuchen gestellt wurde, befunden haben, dass die Überwachung notwendig und verhältnismäßig im Sinne der Konvention ist.

(442) Eine weitere Kontrolle des Regimes zum Informationsaustausch wird durch den GSA gewährt, einen parteiübergreifenden Ausschuss von Mitgliedern des Parlaments mit weiten Befugnissen. [...]

(443) Eine zusätzliche Kontrolle wurde vom ICC geboten, der von der Regierung und den Geheimdiensten unabhängig war. Er war nach § 58 Abs. 4 RIPA verpflichtet, dem Premierminister einen jährlichen Bericht [...] zu erstatten, der dem Parlament vorzulegen war. [...]

(444) Eine letzte Stufe der Kontrolle wird vom IPT gewährt. [...] [Deren Wirksamkeit wurde in der Praxis bereits gezeigt.]

vii. Verhältnismäßigkeit

(446) [...] Der GH akzeptiert, dass das Beziehen einer [klaren] Stellung [gegen jene, die zu Terrorakten beitragen,] und damit die Verhinderung der Verübung gewalttätiger Akte, welche das Leben unschuldiger Personen gefährden, einen Informationsfluss zwischen den Sicherheitsdiensten vieler Länder in allen Teilen der Welt erfordert. Wenn dieser »Informationsfluss« wie im vorliegenden Fall in einen gesetzlichen Rahmen gebettet wurde, der beträchtliche Garantien gegen Missbrauch vorsieht, akzeptiert der GH, dass der daraus resultierende Eingriff auf das beschränkt wurde, was »in einer demokratischen Gesellschaft notwendig« ist.

viii. Ergebnis

(447) Im Lichte der vorangehenden Erwägungen befindet der GH, dass das innerstaatliche Recht zusammen mit den Klarstellungen durch die Änderung des IC Codes das Verfahren für das Ersuchen an ausländische Geheimdienste um Überwachung oder Übermittlung von abgefangenem Material mit ausreichender Deutlichkeit angibt. Diesbezüglich hält er fest, dass die hohe von der Venedig-Kommission empfohlene Schwelle – nämlich dass das übertragene Material nur durchsucht werden können sollte, wenn alle materiellen Voraussetzungen für eine nationale Durchsuchung erfüllt sind und dies ordnungsgemäß und auf die gleiche Weise genehmigt wurde wie die Durchsuchung von Massenmaterial, das von der Signalaufklärungsbehörde unter Verwendung ihrer eigenen Techniken erlangt wurde – vom Regime des belangten Staates erfüllt wird. Der GH

beobachtet weiter, dass es keinen Beweis für wesentliche Mängel bei der Anwendung und Durchführung des Regimes gibt. Ganz im Gegenteil konnte der GSA nach einer Untersuchung überhaupt kein Zeichen von Missbrauch erkennen.

Es erfolgte daher **keine Verletzung** von **Art. 8 EMRK** (5:2 Stimmen; *abweichendes Sondervotum von Richter Koskelo, gefolgt von Richter Turković*).

3. Das Kapitel II-Regime

(450) Die Bf. des zweiten Falles rügten, das Regime zur Erlangung von Kommunikationsdaten unter Kapitel II des RIPA wäre nicht mit ihren Rechten unter Art. 8 EMRK vereinbar.

a. Zulässigkeit

(451) [...] Die Regierung brachte vor, die Bf. wären nicht Opfer der gerügten Verletzung iSd. Art. 34 EMRK.

(453) Die Bf. können nur behaupten, schon aufgrund der Existenz des Regimes nach Kapitel II Opfer zu sein, wenn sie zeigen können, dass sie aufgrund ihrer persönlichen Situation potentiell Gefahr liefen, dass ihre Kommunikationsdaten durch die Behörden des Vereinigten Königreichs über Ersuchen an einen KDL erlangt wurden.

(454) Diesbezüglich bemerkt der GH, dass das Regime nach Kapitel II kein Regime zur massenweisen Erlangung von Kommunikationsdaten ist, sondern [...] es Behörden erlaubt, spezielle Kommunikationsdaten zu verlangen. Trotzdem ist eine große Zahl an Behörden befugt, solche Ersuchen zu stellen, und die Gründe, aus denen ein Ersuchen gestellt werden kann, sind relativ weit. Nachdem die Bf. des zweiten Falles Investigativjournalisten sind, die über Themen wie CIA-Folter, Terrorismusbekämpfung, Drohnenkrieg und die irakischen Kriegstagebücher berichteten, akzeptiert der GH, dass sie potentiell Gefahr liefen, dass die Behörden des Vereinigten Königreichs ihre Kommunikation erlangen, entweder direkt, indem sie einen KDL um die Kommunikationsdaten ersuchen, oder indirekt, indem sie einen KDL um die Kommunikationsdaten einer Person oder Organisation ersuchen, mit der sie in Kontakt gestanden waren.

(455) Der GH akzeptiert daher, dass sie [...] Opfer iSd. Konvention waren. Da diese Beschwerde auch nicht aus anderen Gründen unzulässig ist, muss sie für **zulässig** erklärt werden (mehrheitlich).

b. In der Sache

(466) Der GH beobachtet, dass das Kapitel II-Regime in § 22 RIPA und dem ACD Code eine eindeutige Grundlage hat. Da das Vereinigte Königreich jedoch ein Mitgliedstaat der EU ist, ist die Rechtsordnung der Gemeinschaft in jene des Vereinigten Königreichs integriert, und wenn es einen Konflikt zwischen dem innerstaatlichen Recht und dem EU-Recht gibt, hat Letzteres Vorrang. Konsequenterweise hat die Regierung zugestanden, dass Teil 4 des IPA mit dem EU-Recht unvereinbar war, weil der Zugang zu gespeicherten Daten nicht auf den Zweck der Bekämpfung »schwerwiegender Verbrechen« eingeschränkt und der Zugang zu gespeicherten Daten keiner vorangehenden Überprüfung durch ein Gericht oder unabhängiges Verwaltungsorgan unterworfen war. Nach diesem Eingeständnis ordnete der *High Court* an, dass die einschlägigen Bestimmungen des IPA mit 1.11.2018 geändert werden sollten.

(467) [...] Da das Kapitel II-Regime Zugang zu gespeicherten Daten zum Zweck der Bekämpfung von Verbrechen (statt »schwerwiegender Verbrechen«) erlaubt und außer für den Zugang zum Zweck der Bestimmung einer journalistischen Quelle keiner vorherigen Überprüfung durch ein Gericht oder unabhängiges Verwaltungsorgan unterworfen ist, kann es nicht iSd. Art. 8 EMRK gesetzlich vorgesehen sein.

(468) Es erfolgte daher eine **Verletzung** von **Art. 8 EMRK** (6:1 Stimmen; *abweichendes Sondervotum von Richterin Pardalos*).

III. Zur behaupteten Verletzung von Art. 10 EMRK

1. Zulässigkeit

(471-474) [Was die Bf. des dritten Falles angeht, so haben diese im Hinblick auf einen Teil der Rügen den innerstaatlichen Instanzenzug nicht erschöpft. Ihre Beschwerde muss deshalb diesbezüglich für **unzulässig** erklärt werden (einstimmig). Im Hinblick auf die übrigen von ihnen erhobenen Rügen ist eine gesonderte Prüfung nicht notwendig, da dadurch keine Fragen aufgeworfen werden, die über die unter Art. 8 EMRK behandelten hinausgehen.]

(475) Da der GH anerkannt hat, dass die Bf. des zweiten Falles ausnahmsweise vom Erfordernis befreit waren, ihre Rügen zunächst an das IPT heranzutragen [siehe oben Rn. 268], kann nicht gesagt werden, dass sie es verabsäumt hätten, den Instanzenzug [...] zu erschöpfen. Nachdem ihre Rügen auch nicht aus anderen Gründen unzulässig sind, müssen sie daher für **zulässig** erklärt werden (mehrheitlich).

(476) Bei den Bf. des zweiten Falles handelt es sich außerdem um einen Journalisten und eine Organisation, die Nachrichten sammelt, die sich über den Eingriff in vertrauliches journalistisches Material durch den Betrieb sowohl des § 8 Abs. 4-Regimes als auch des Kapitel II-Regimes beschweren. Deshalb werfen ihre Beschwerden im Vergleich zu jenen unter Art. 8 EMRK gesonderte Fragen auf [...].

2. In der Sache

a. Das § 8 Abs. 4-Regime

(492) Was die Notwendigkeit betrifft, wiederholt der GH, dass ein Eingriff unter Berücksichtigung der Bedeutung des Schutzes journalistischer Quellen für die Pressefreiheit in einer demokratischen Gesellschaft nicht im Einklang mit Art. 10 EMRK stehen kann, wenn er nicht durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt ist. Diesbezüglich bemerkt er, dass die Überwachungsmaßnahmen nach dem § 8 Abs. 4-Regime [...] nicht darauf abzielen, Journalisten zu überwachen oder journalistische Quellen offenzulegen. Allgemein wissen die Behörden erst, ob die Kommunikation eines Journalisten abgefangen wurde, wenn sie die abgefangene Kommunikation prüfen. Daher bestätigt er, dass das Abfangen solcher Kommunikationen nicht bereits für sich als ein besonders schwerer Eingriff in die Meinungsäußerungsfreiheit charakterisiert werden kann. Der Eingriff wird jedoch stärker, wenn diese Kommunikation zur Prüfung ausgewählt wird. Er kann nach Ansicht des GH nur »durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt« sein, wenn er von ausreichenden Garantien begleitet wird, und zwar sowohl im Hinblick auf die Umstände, unter denen sie bewusst zur Prüfung ausgewählt werden darf, als auch im Hinblick auf den Schutz der Vertraulichkeit, wenn sie – sei es bewusst oder nicht – zur Prüfung ausgewählt wurde.

(493) Diesbezüglich verlangen die §§ 4.1-4.8 des IC Codes eine spezielle Berücksichtigung der Überwachung von Kommunikationen, die vertrauliches journalistisches Material und vertrauliche persönliche Informationen betreffen. Diese Bestimmungen scheinen sich jedoch nur auf die Entscheidung zur Ausstellung einer Überwachungsermächtigung zu beziehen. Deshalb mögen sie zwar angemessene Garantien im Hinblick auf eine gezielte Ermächtigung unter § 8 Abs. 1 RIPA bieten, scheinen aber keine Bedeutung für ein Regime der Massenüberwachung zu haben. Zudem hat der GH bereits die fehlende Transparenz und Kontrolle der Kriterien für die Durchsuchung und Auswahl von Kommunikation zur Prüfung kritisiert (siehe oben Rn. 339, 340, 345 und 387). Im Kontext des Art. 10 EMRK ist es von besonderem Interesse, dass es keine Voraussetzungen für die Befugnis der Geheimdienste gibt, nach vertraulichem journalistischem oder anderem Material zu suchen (z.B. durch die Verwendung der Emailadresse eines Journalisten als Auswahlkriterium), oder Anforderungen, die von Analysten verlangen, bei der Auswahl von Material zur Prüfung besonders zu beachten, ob solches Material betroffen ist oder sein kann. Folglich scheint es, dass Analysten sowohl den Inhalt als auch die dazugehörigen Kommunikationsdaten dieser abgefangenen Kommunikation ohne Beschränkung durchsuchen und prüfen konnten.

(495) [...] Angesichts der potentiellen abschreckenden Wirkung, die jeder wahrgenommene Eingriff in die Vertraulichkeit ihrer Kommunikation und insbesondere ihrer Quellen auf die Freiheit der Presse haben kann, und des Fehlens irgendwelcher [...] Vorkehrungen, die die Möglichkeit der Geheimdienste eingrenzen, solches Material zu durchsuchen und zu prüfen, auch wenn es nicht »durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt ist«, stellt der GH fest, dass auch eine Verletzung von Art. 10 EMRK erfolgte.

b. Das Kapitel II-Regime

(498) Der GH anerkennt, dass das Kapitel II-Regime einen verstärkten Schutz gewährt, wenn Daten mit dem Zweck begehrt werden, eine journalistische Quelle zu identifizieren. Insbesondere sieht § 3.77 des ACD Codes vor, dass dann, wenn ein Antrag beabsichtigt, die Quelle einer journalistischen Information zu bestimmen, ein vorrangiges Erfordernis im öffentlichen Interesse gegeben sein muss und solche Anträge das Verfahren des Polizei- und Strafrechtlichen Beweisgesetzes (*Police and Criminal Evidence Act*) verwenden müssen, bei einem Gericht eine Herausgabeanordnung zur Erlangung dieser Daten zu beantragen. [...] Wenn der Antrag sich auf journalistisches Material [...] bezieht, [...] hat der Antrag *inter partes* zu erfolgen. [...]

(499) Dennoch finden diese Bestimmungen nur Anwendung, wenn es der Zweck des Antrags ist, eine Quelle zu bestimmen, nicht aber in jedem Fall, in dem um die Kommunikationsdaten eines Journalisten ersucht wird oder ein solcher begleitender Eingriff wahrscheinlich ist. Zudem gibt es in Fällen betreffend den Zugang zu den Kommunikationsdaten eines Journalisten keine speziellen Bestimmungen, die den Zugang auf den Zweck der Bekämpfung »schwerwiegender Verbrechen« beschränken. Folglich erwägt der GH, dass das Regime nicht »gesetzlich vorgesehen« [...] ist.

c. Gesamtschlussfolgerung

(500) [...] Der GH stellt [...] eine **Verletzung** von **Art. 10 EMRK** fest (6:1 Stimmen; *abweichendes Sondervotum von Richterin Pardalos*).

IV. Zur behaupteten Verletzung von Art. 6 EMRK

(506) Bislang haben weder die EKMR noch der GH befunden, dass Art. 6 Abs. 1 EMRK auf Verfahren Anwendung findet, die eine Entscheidung betreffen, eine Person unter Überwachung zu stellen. [...]

(508) Im vorliegenden Fall ist es für den GH [...] nicht nötig, eine fundierte Schlussfolgerung zur Frage der

Anwendbarkeit von Art. 6 EMRK zu treffen, da er aus den unten angeführten Gründen befindet, dass die Rüge der Bf. offensichtlich unbegründet ist.

(509) Was die allgemeinen Rügen der Bf. betreffend das Verfahren vor dem IPT angeht, einschließlich der Beschränkungen der Offenlegung [von Informationen] und der Abhaltung von öffentlichen Verhandlungen im Interesse der nationalen Sicherheit, erinnert der GH daran, dass im Fall *Kennedy/GB* ähnliche Rügen erhoben wurden. Dort kam der GH unter Berücksichtigung der einschlägigen Verfahrensbestimmungen zum Schluss, dass die Beschränkungen der Verfahrensrechte des Bf. zur Sicherstellung der Wirksamkeit des geheimen Überwachungsregimes [...] sowohl notwendig als auch verhältnismäßig waren und das Wesen seiner Rechte unter Art. 6 EMRK nicht beeinträchtigten.

(510) Der GH sieht keinen Grund, im vorliegenden Fall zu einem anderen Ergebnis zu kommen. Er hat oben in den Rn. 250-265 bereits festgehalten, dass mit der umfassenden Befugnis des IPT, Beschwerden betreffend den unrechtmäßigen Eingriff in Kommunikation nach dem RIPA zu prüfen, ein wirksames Rechtsmittel existierte, das in Theorie und Praxis zur Verfügung stand und geeignet war, Personen Wiedergutmachung zu gewähren, die sich über spezielle Fälle von Überwachung oder die allgemeine Konventionskonformität eines Überwachungsregimes beschwerten. Zudem wurde diese umfassende Befugnis im Fall der Bf. eingesetzt, um die Fairness des Verfahrens sicherzustellen: Insbesondere wurde sämtliches relevantes (freigegebenes und gesperrtes) Material durch das IPT geprüft; wurde den Bf. Material nur dann vorenthalten, wenn das IPT überzeugt war, dass es angemessene öffentliche Interessen und Gründe der nationalen Sicherheit dafür gab; und bestellte das IPT schließlich einen *Counsel to the Tribunal*, um im nichtöffentlichen Verfahren Eingaben im Namen der Bf. zu tätigen.

(513) Aus diesem Grund befindet der GH, dass die Rüge unter Art. 6 Abs. 1 EMRK als offensichtlich unbegründet [...] [und daher **unzulässig**] zurückzuweisen ist (einstimmig).

V. Entschädigung nach Art. 41 EMRK

€ 150.000,– an die Bf. des ersten Falles, € 35.000,– an die Bf. des zweiten Falles für Kosten und Auslagen (6:1 Stimmen).