Big Brother Watch u.a. gg. das Vereinigte Königreich – 58170/13 u.a.

Urteil vom 25.5.2021, Große Kammer

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. Aus den Enthüllungen ergab sich, dass das *Government Communications Headquarter* (»GCHQ«, einer der Geheimdienste des Vereinigten Königreichs) 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 Kommunikationsdienstleister gesammelt. Gerade durch letztgenanntes Programm bestand ein weitreichender Zugang auch auf Daten von nichtamerikanischen Staatsbürgern.

Die 16 Bf. halten es für wahrscheinlich, dass ihre elektronische Kommunikation aufgrund ihrer Aktivitäten (bei ihnen handelt es sich um Journalisten oder Personen bzw. Organisationen, die sich für Bürgerrechte einsetzen) entweder (1) von den Geheimdiensten des Vereinigten Königreichs unter dem Regime des damaligen § 8 Abs. 4 des Gesetzes über Ermittlungsbefugnisse (*Regulation of Investigatory Powers Act 2000*, im Folgenden: »RIPA«) direkt überwacht wurde;[1] (2) von ausländischen Regierungen überwacht und das erlangte Material dann an die Geheimdienste des Vereinigten Königreichs weitergegeben wurde und/oder (3) durch die Behörden des Vereinigten Königreichs nach Kapitel II des RIPA von Kommunikationsdienstleistern erlangt wurde.

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 sah auch einen sogenannten Beauftragten für die Kom-

1 Demzufolge konnte der *Secretary of State* zu einer Überwachung grenzüberschreitender Kommunikationen über ein Telekommunikationssystem ermächtigen, wobei er auch eine Bescheinigung auszustellen hatte, die das für eine Auswertung relevante Material umschrieb und erläuterte, warum die Auswertung im Interesse der nationalen Sicherheit, zur Verhütung oder Aufklärung schwerer Verbrechen oder zum Schutz des wirtschaftlichen Wohls des Vereinigten Königreichs notwendig war.

munikationsüberwachung (*Interception of Communications Commissioner*, im Folgenden: »ICC«) vor, der eine unabhängige Kontrolle der Wahrnehmung der Befugnisse und Pflichten unter diesem Gesetz zu gewährleisten hatte. Das RIPA wurde später durch den *Investigatory Powers Act* (»IPA«) 2016 teilweise ersetzt.

Rechtsausführungen

Die Bf. rügten eine Verletzung von Art. 8 EMRK (hier: *Recht auf Achtung des Privatlebens*) und von Art. 10 EMRK (*Meinungsäußerungsfreiheit*) durch die genannten drei Regime.

I. Vorfrage vor der Großen Kammer

(269) Die Bf. erhoben ihre Beschwerden 2013, 2014 bzw. 2015. Diese betrafen hauptsächlich die staatlichen Überwachungsaktivitäten unter dem RIPA und den damit verbundenen *Codes of Practice*. Letztere wurden in der Folge geändert. Was noch wichtiger ist: […] Das neue Überwachungsregime nach dem IPA 2016 trat größtenteils im Sommer 2018 in Kraft. Die Bestimmungen des Kapitels I Teil I des RIPA [zu dem auch § 8 Abs. 4 gehörte] wurden […] aufgehoben.

(270) Die Kammer untersuchte die Konventionskonformität des Rechts, das zu dem Zeitpunkt in Kraft stand, als sie die Zulässigkeit der Beschwerden prüfte. Sie berücksichtigte daher die Rechtslage am 7.11.2017. Da dies die »Rechtssache« darstellt, »wie sie für zulässig erklärt wurde«, muss die GK ihre Untersuchung ebenso auf die Rechtslage am 7.11.2017 beschränken. Dies ist angebracht, da die rechtlichen Regime, die nach dem Inkrafttreten des IPA schrittweise eingefügt wurden, aktuell vor den innerstaatlichen Gerichten angefochten werden und es der GK nicht offenstehen würde, die neue Gesetzgebung zu prüfen, bevor diese Gerichte die Gelegenheit dazu hatten.

II. Zur Massenüberwachung von Kommunikationen nach § 8 Abs. 4 RIPA

1. Zur behaupteten Verletzung von Art. 8 EMRK

(324) Die Regierung bestreitet nicht, dass ein **Eingriff** in die Rechte der Bf. nach Art. 8 EMRK erfolgte […].

(325) Der GH sieht Massenüberwachung als einen schrittweisen Prozess, bei dem der Grad des Eingriffs in die Rechte von Individuen nach Art. 8 EMRK zunimmt, je weiter der Prozess voranschreitet. Regime zur Massenüberwachung mögen nicht alle genau demselben Muster folgen und die verschiedenen Etappen des Prozesses werden nicht notwendig separat oder streng chronologisch erfolgen. Unter Beachtung dieser Vorbehalte befindet der GH dennoch, dass die folgenden Phasen dieses Prozesses zu berücksichtigen sind:

(a) die Überwachung und anfängliche Speicherung von Kommunikationen und dazugehörigen Kommunikationsdaten (das sind die Verkehrsdaten im Zusammenhang mit der überwachten Kommunikation);

(b) die Anwendung spezieller Selektoren auf die gespeicherten Kommunikationen bzw. […] Kommunikationsdaten;

(c) die Auswertung ausgewählter Kommunikationen bzw. […] Kommunikationsdaten durch Analysten; und

(d) die nachfolgende Speicherung von Daten und Verwendung des »Endprodukts«, einschließlich des Teilens von Daten mit Dritten.

(326) [Zu (a):] […] Elektronische Kommunikationen […] werden von den Geheimdiensten massenweise überwacht. Sie werden zu einer großen Zahl Individuen betreffen, von denen viele für die Geheimdienste völlig uninteressant sind. Kommunikationen, an denen wahrscheinlich kein geheimdienstliches Interesse besteht, können in dieser Phase herausgefiltert werden.

(327) [Zu (b):] Die anfängliche Durchsuchung, die meist automatisch erfolgt, findet statt […], wenn verschiedene Arten von Selektoren […] auf die gespeicherten Pakte von Kommunikationen und zugehörigen Kommunikationsdaten angewendet werden. Das kann die Phase sein, wo der Prozess durch die Verwendung von starken Selektoren [wie z.B. Emailadressen] erstmals auf Individuen abzielt.

(328) [Zu (c):] […] Abgefangenes Material wird [in dieser Phase] zum ersten Mal von einem Analysten ausgewertet.

(329) [Zu (d):] […] Das abgefangene Material wird von den Geheimdiensten tatsächlich verwendet. Das kann die Erstellung eines Geheimdienstberichts, die Weitergabe des Materials an andere Geheimdienste innerhalb des Staates oder auch die Weitergabe von Material an ausländische Geheimdienste umfassen.

(330) Art. 8 EMRK ist auf jede der oben genannten Phasen anzuwenden. Während die anfängliche Überwachung, der unmittelbar die Löschung von Teilen der Kommunikation folgt, keinen erheblichen Eingriff darstellt, wird der Grad des Eingriffs in die Rechte der Individuen nach Art. 8 EMRK steigen, je weiter das Verfahren zur Massenüberwachung voranschreitet. In diesem Zusammenhang hat der GH bereits eindeutig festgehalten, dass schon das bloße Speichern von auf das Privatleben bezogenen Daten eines Individuums einen Eingriff iSv. Art. 8 EMRK darstellt (*Leander/S*) und dass die Notwendigkeit von Garantien umso größer sein wird, wenn der Schutz persönlicher Daten betroffen ist, die einer automatischen Verarbeitung unterzogen werden (*S. und Marper/GB*). […] Am Ende des Prozesses schließlich, wenn die Informationen über eine bestimmte Person analysiert werden oder der Inhalt der Kommunika-

tionen durch einen Analysten untersucht wird, wird die Notwendigkeit für Garantien am höchsten sein. [...]

(335) [Im Zusammenhang mit der **Rechtfertigung des Eingriffs**] ist daran zu erinnern, dass der GH in seiner Rechtsprechung zur Überwachung von Kommunikation bei strafrechtlichen Ermittlungen folgende Anforderungen entwickelt hat, die im Gesetz mindestens festzulegen sind, um Machtmissbrauch zu vermeiden: (i) die Natur der Straftaten, die eine Überwachungsanordnung bewirken können; (ii) eine Definition der Personenkategorien, die einer Überwachung ihrer Kommunikation ausgesetzt sein können; (iii) eine Begrenzung der Dauer der Überwachung; (iv) das bei der Auswertung, Verwendung und Speicherung der erlangten Daten einzuhaltende Verfahren; (v) die zu treffenden Vorkehrungen, wenn die Daten an andere übermittelt werden; und (vi) die Umstände, unter denen abgefangene Daten gelöscht oder zerstört werden können oder müssen [...].

(338) Bei der Frage, ob ein Eingriff zur Verfolgung eines legitimen Ziels »in einer demokratischen Gesellschaft notwendig war«, hat der GH 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.

a. Besteht eine Notwendigkeit, die Rechtsprechung weiterzuentwickeln?

(340) In *Weber und Saravia/D* und *Liberty u.a./GB* akzeptierte der GH, dass Regime zur Massenüberwachung nicht per se aus dem Ermessensspielraum der Staaten herausfallen. Angesichts der Verbreitung von Bedrohungen, denen Staaten aktuell durch Netzwerke internationaler Akteure ausgesetzt sind, die das Internet zur Kommunikation und als Werkzeug verwenden, und der Existenz ausgeklügelter Technologie, die es diesen Akteuren ermöglicht, eine Entdeckung zu vermeiden, befindet der GH, dass die Entscheidung, ein Regime zur Massenüberwachung zu betreiben, um Bedrohungen für die nationale Sicherheit oder wesentliche nationale Interessen zu identifizieren, weiterhin in diesen Ermessensspielraum fällt.

(341) Sowohl in *Weber und Saravia/D* als auch in *Liberty u.a./GB* wendete der GH [...] sechs Mindestgarantien an, die in seiner Rechtsprechung zu zielgerichteter Überwachung entwickelt worden waren (siehe Rn. 335 oben). Auch wenn die Regime zur Massenüberwachung, die in diesen Fällen geprüft wurden, auf den ersten Blick ähnlich zu jenem waren, das im vorliegenden Fall in Frage steht, so sind beide Fälle mittlerweile mehr als zehn Jahre alt, während die technologischen Entwicklungen zwischenzeitlich die Art und Weise, wie Personen kommunizieren, bedeutend geändert haben. Das Leben findet vermehrt online statt und generiert eine wesentliche größere Menge an elektronischer Kommunikation sowie Kommunikation mit einer erheblich veränderten Natur und Qualität [...]. Die Reichweite der in diesen Fällen untersuchten Überwachungsaktivität war daher viel geringer.

(342) Das gilt gleichermaßen für zugehörige Kommunikationsdaten. [...] Aktuell sind im Vergleich zu Inhaltsdaten größere Mengen an Kommunikationsdaten zu einem Individuum verfügbar, da jeder Inhalt mit mehreren Kommunikationsdaten verbunden ist. Während der Inhalt verschlüsselt sein und jedenfalls nichts Wesentliches über den Absender oder Empfänger enthüllen mag, können die zugehörigen Kommunikationsdaten eine große Menge an persönlichen Informationen offenlegen, wie Identität und Standort von Absender und Empfänger, sowie Informationen über die Einrichtung, über welche die Kommunikation übermittelt wurde. Zudem ist jeder Eingriff durch die Erlangung von [...] Kommunikationsdaten verstärkt, wenn sie massenweise erlangt werden, da sie dann auf eine Weise analysiert und abgefragt werden können, die es ermöglicht, ein persönliches Bild von einer Person zu zeichnen, indem deren Aktivitäten in den sozialen Netzwerken, deren Fortbewegungen, deren Internetsurfverhalten und deren Kommunikationsgewohnheiten nachverfolgt werden sowie Kenntnis von deren Kontakten erlangt wird.

(343) Am wesentlichsten ist jedoch, dass der GH in *Weber und Saravia/D* und *Liberty u.a./GB* den Umstand nicht ausdrücklich ansprach, dass er sich mit einer Überwachung befasste, die im Vergleich zu früheren Fällen im Hinblick auf Natur und Ausmaß verschieden war. Allerdings unterscheiden sich eine gezielte Überwachung und eine Massenüberwachung in mehrerlei Hinsicht.

(344) Zunächst ist Massenüberwachung allgemein auf internationale Kommunikationen gerichtet (also Kommunikationen, die physisch über Staatsgrenzen hinweggehen). Während die Überwachung und sogar Auswertung von Kommunikationen von Personen innerhalb des überwachenden Staates nicht ausgeschlossen sein mag, so ist in vielen Fällen die erklärte Absicht von Massenüberwachung, die Kommunikationen von Personen zu überwachen, die sich außerhalb der territorialen Hoheitsgewalt des Staates befinden und die daher nicht durch andere Methoden überwacht werden können. [...]

(345) Zudem scheinen [...] die Zwecke, für die Massenüberwachung eingesetzt werden kann, unterschiedlich zu sein. Soweit der GH gezielte Überwachungen untersucht hat, wurden diese vom belangten Staat meist zur Ermittlung im Zusammenhang mit Verbrechen eingesetzt. Mag Massenüberwachung auch verwendet werden, um gewisse schwerwiegende Verbrechen zu untersuchen, scheinen sie die Mitgliedstaaten des Europarats [...] zur Sammlung ausländischer Informationen, die Früherkennung von Cyberattacken und diesbezügliche Ermittlungen, Spionageabwehr und Terrorismus-

bekämpfung einzusetzen.

(346) Während Massenüberwachung nicht notwendig im Hinblick auf konkrete Individuen eingesetzt wird, kann sie offenkundig für diesen Zweck herangezogen werden und wird dies auch. In einem solchen Fall werden jedoch die Geräte der Zielpersonen nicht überwacht. Vielmehr werden diese durch die Anwendung starker Selektoren […] auf die von den Geheimdiensten massenweise abgefangene Kommunikation anvisiert. Es werden nur diejenigen Kommunikationspakete des betroffenen Individuums, die die Übertragungsleitungen durchliefen, die von den Geheimdiensten ausgewählt wurden, auf diese Weise abgefangen, und nur die Kommunikation, die entweder eine Übereinstimmung mit einem starken Selektor oder einer komplexen Abfrage aufwies, kann von einem Analysten untersucht werden.

(347) Wie jedes Überwachungsregime hat auch Massenüberwachung ein beträchtliches Potential, auf eine Weise missbraucht zu werden, die das Recht von Individuen auf Achtung des Privatlebens beeinträchtigt. Während Art. 8 EMRK den Einsatz von Massenüberwachung nicht verbietet, um die nationale Sicherheit und andere essentielle nationale Interessen vor schwerwiegenden externen Bedrohungen zu schützen, und die Staaten ein weites Ermessen bei der Entscheidung genießen, welche Art von Überwachungsregime für diese Zwecke notwendig ist, muss der ihnen gewährte Ermessensspielraum beim Betrieb eines solchen Systems kleiner sein. Zudem muss eine Reihe von Garantien vorgesehen sein, wobei der GH bereits bestimmt hat, mit welchen Garantien ein konventionskonformes Regime gezielter Überwachung ausgestattet sein sollte. Während diese Grundsätze einen nützlichen Rahmen bieten, müssen sie angepasst werden, um die speziellen Merkmale eines Regimes zur Massenüberwachung und insbesondere den zunehmenden Grad des Eingriffs in die Rechte der Individuen nach Art. 8 EMRK zu reflektieren, wenn der Vorgang die in Rn. 325 oben identifizierten Phasen durchläuft.

b. Der in Fällen von Massenüberwachung zu verfolgende Ansatz

(348) Es ist klar, dass die ersten beiden der sechs »Mindestgarantien«, die der GH im Zusammenhang mit gezielter Überwachung festgelegt hat, […] nicht ohne Weiteres auf ein Regime der Massenüberwachung anwendbar sind […]. Ähnlich ist das Erfordernis eines »begründeten Verdachts« […] im Kontext einer Massenüberwachung weniger relevant, deren Zweck grundsätzlich präventiv ist […]. Dennoch erachtet es der GH für zwingend erforderlich, dass wenn ein Staat ein solches Regime betreibt, das innerstaatliche Recht detaillierte Regelungen dahingehend enthalten muss, wann die Behörden auf solche Maßnahmen zurückgreifen dürfen. Insbesondere muss das innerstaatliche Recht mit ausreichender Klarheit die Gründe darlegen, aus denen eine Massenüberwachung genehmigt werden darf, und die Umstände, unter denen die Kommunikation eines Individuums überwacht werden kann. Die übrigen vier Mindestgarantien […] sind gleichermaßen für Massenüberwachungen relevant.

(349) In seiner Rechtsprechung zu gezielter Überwachung hat der GH Vorkehrungen für die Beaufsichtigung und Überprüfung des Überwachungsregimes berücksichtigt. Im Kontext von Massenüberwachung ist die Bedeutung von Beaufsichtigung und Überprüfung größer, weil ein immanentes Risiko von Missbrauch besteht und das berechtigte Bedürfnis von Geheimhaltung unvermeidbarerweise bedeutet, dass Staaten aus Gründen der nationalen Sicherheit oft nicht frei sein werden, Informationen im Zusammenhang mit dem Betrieb des strittigen Regimes preiszugeben.

(350) Daher ist der GH der Ansicht, dass […] der Prozess »durchgehenden Garantien« unterworfen werden muss. Das bedeutet, dass auf innerstaatlicher Ebene in jeder Phase des Prozesses eine Beurteilung der Notwendigkeit und Verhältnismäßigkeit der gesetzten Maßnahmen vorgenommen werden muss; dass Massenüberwachung zu Beginn einer unabhängigen Genehmigung zu unterwerfen ist, wenn Ziel und Umfang der Operation festgelegt werden; und dass die Operation einer Kontrolle und unabhängigen *ex post facto*-Überprüfung unterworfen werden muss. Nach Ansicht des GH sind dies grundlegende Garantien, die Eckpfeiler jedes mit Art. 8 EMRK im Einklang stehenden Regimes zur Massenüberwachung bilden müssen […].

(351) Was zunächst die Genehmigung betrifft, so stimmt die GK der Kammer zu, dass während eine richterliche Genehmigung eine »wichtige Garantie gegen Willkür« ist, sie kein »notwendiges Erfordernis« darstellt. Dennoch sollte die Massenüberwachung durch ein von der Exekutive unabhängiges Organ genehmigt werden.

(352) Zudem sollte das unabhängige genehmigende Organ […] sowohl vom Zweck der Überwachung als auch den vermutlich zu überwachenden Übertragungsleitungen oder Kommunikationswegen informiert werden. Das würde es ihm ermöglichen, die Notwendigkeit und Verhältnismäßigkeit der Operation zur Massenüberwachung zu beurteilen und auch, ob die Auswahl der Übertragungsleitungen zu den Zwecken der Überwachung notwendig und verhältnismäßig ist.

(353) Die Verwendung von Selektoren – und insbesondere von starken Selektoren – ist im Prozess der Massenüberwachung einer der wichtigsten Schritte, da dies der Punkt ist, an dem die Kommunikationen eines bestimmten Individuums von den Geheimdiensten anvisiert werden können. Während jedoch manche Systeme die vorherige Genehmigung von Kategori-

en von Selektoren vorsehen [...], bemerkt der GH, dass die Regierungen des Vereinigten Königreichs und der Niederlande vorgebracht haben, dass jedes Erfordernis, Selektoren oder Suchkriterien in der Genehmigung zu erläutern oder zu begründen, die Wirksamkeit von Massenüberwachung ernsthaft beschränken würde. Das wurde auch vom IPT akzeptiert [...].

(354) Unter Berücksichtigung der Charakteristika von Massenüberwachung, der großen Zahl an verwendeten Selektoren und des immanenten Bedürfnisses nach Flexibilität bei der Wahl der Selektoren [...] akzeptiert der GH, dass die Einbeziehung aller Selektoren in die Genehmigung in der Praxis nicht machbar sein mag. Dennoch sollte die Genehmigung – da die Wahl von Selektoren und Suchbegriffen bestimmt, welche Kommunikationen für die Auswertung durch einen Analysten in Frage kommen – zumindest die Arten oder Kategorien der zu verwendenden Selektoren bezeichnen.

(355) Zudem sollten verstärkte Garantien eingerichtet sein, wenn von den Geheimdiensten starke Selektoren angewendet werden, die mit identifizierbaren Individuen in Zusammenhang stehen. Die Verwendung eines jeden solchen Selektors muss von den Geheimdiensten im Hinblick auf die Grundsätze der Notwendigkeit und Verhältnismäßigkeit gerechtfertigt werden und diese Rechtfertigung muss genau dokumentiert und einem Verfahren vorheriger interner Genehmigung unterworfen werden, das eine gesonderte und objektive Prüfung der Frage bietet, ob die Rechtfertigung den vorgenannten Grundsätzen entspricht.

(356) Jede Phase des Massenüberwachungsprozesses [...] muss auch der Beaufsichtigung durch eine unabhängige Behörde unterworfen sein, die ausreichend stark sein muss, um den Eingriff auf das »in einer demokratischen Gesellschaft Notwendige« zu beschränken. Insbesondere muss das beaufsichtigende Organ in der Lage sein, die Notwendigkeit und Verhältnismäßigkeit der gesetzten Handlung zu beurteilen. Dabei ist der Grad des Eingriffs in Konventionsrechte der Personen, die vermutlich betroffen sein werden, gebührend zu berücksichtigen. Um diese Beaufsichtigung zu erleichtern, sollten von den Geheimdiensten in jedem Stadium des Prozesses detaillierte Aufzeichnungen geführt werden.

(357) Schließlich muss jedem, der Verdacht schöpft, dass seine Kommunikation geheimdienstlich überwacht wird, ein wirksames Rechtsmittel zur Verfügung stehen, um entweder die Rechtmäßigkeit der vermuteten Überwachung oder die Konventionskonformität des Überwachungsregimes in Frage zu stellen. [...]

(358) Auch ein Rechtsbehelf, der nicht von der Benachrichtigung einer Zielperson abhängt, kann im Zusammenhang mit Massenüberwachungen ein wirksamer Rechtsbehelf sein. Tatsächlich kann er, abhängig von den Umständen, sogar bessere Garantien für eine korrekte Vorgehensweise bieten als ein System, das auf einer Benachrichtigung beruht. Ungeachtet dessen, ob Material durch gezielte oder Massenüberwachung erlangt wurde, kann die Existenz einer Ausnahme wegen der nationalen Sicherheit ein Erfordernis der Benachrichtigung jeder praktischen Wirkung berauben. Die Wahrscheinlichkeit, dass das Erfordernis einer Benachrichtigung eine bloß geringe oder gar keine praktische Wirkung hat, wird im Zusammenhang mit Massenüberwachung höher sein, da eine solche Überwachung zum Zwecke der Sammlung ausländischer Geheimdienstinformationen verwendet werden kann und größtenteils auf die Kommunikation von Personen außerhalb der Hoheitsgewalt des Staates abzielen wird. Deshalb kann den Behörden, auch wenn ihnen die Identität einer Zielperson bekannt ist, deren Standort unbekannt sein.

(359) Die Befugnisse und prozessualen Garantien, über die eine Behörde verfügt, sind bei der Beurteilung von Relevanz, ob ein Rechtsbehelf wirksam ist. Daher ist es bei Fehlen eines Benachrichtigungserfordernisses unerlässlich, dass der Rechtsbehelf vor einem Organ erhoben können werden muss, das wenn auch nicht notwendig richterlich, so doch von der Exekutive unabhängig ist, die Fairness des Verfahrens sicherstellt und soweit als möglich ein kontradiktorisches Verfahren bietet. Die Entscheidungen eines solchen Organs müssen begründet und im Hinblick auf unter anderem die Beendigung einer unrechtmäßigen Überwachung und der Löschung von unrechtmäßig erlangtem und/oder aufbewahrtem Material rechtlich verbindlich sein [...].

(360) Vor dem Hintergrund des Vorgesagten wird der GH darüber entscheiden, ob ein Regime zur Massenüberwachung konventionskonform ist, indem er eine Gesamtbeurteilung der Anwendung des Regimes vornimmt. Eine solche Beurteilung wird sich primär darauf konzentrieren, ob der innerstaatliche Rechtsrahmen ausreichende Garantien gegen Missbrauch enthält und ob das Verfahren mit »durchgehenden Garantien« versehen ist (siehe Rn. 350 oben). Dabei wird er die tatsächliche Anwendung des Überwachungssystems berücksichtigen, einschließlich der »Checks and Balances« im Hinblick auf die Ausübung der Befugnis, und die Existenz oder das Fehlen irgendeines Beweises für tatsächlichen Missbrauch.

(361) Bei der Beurteilung, ob der belangte Staat innerhalb seines Ermessensspielraumes agierte, hat der GH eine größere Bandbreite an Kriterien zu berücksichtigen als die sechs *Weber*-Garantien. Genauer gesagt wird der GH [...] prüfen, ob der innerstaatliche Rechtsrahmen eindeutig festlegte:

1. die Gründe, aus denen eine Massenüberwachung genehmigt werden darf;

2. die Umstände, unter denen die Kommunikation eines Individuums überwacht werden darf;

3. das für die Gewährung der Genehmigung einzu-

haltende Verfahren;

4. die für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltenden Verfahren;

5. die zu treffenden Vorkehrungen, wenn das Material an andere Parteien übermittelt wird;

6. die Grenzen für die Dauer der Überwachung und Aufbewahrung von abgefangenem Material und die Umstände, unter denen solches Material gelöscht und zerstört werden muss;

7. die Verfahren und Modalitäten für die Kontrolle durch eine unabhängige Behörde im Hinblick auf die Einhaltung der obigen Garantien und deren Befugnisse im Falle der Nichteinhaltung;

8. das Verfahren für eine unabhängige *ex post facto*-Überprüfung der Einhaltung und die Befugnisse des zuständigen Organs für den Fall der Nichteinhaltung.

(362) Obwohl es sich dabei um eines der sechs *Weber*-Kriterien handelt, hat der GH bislang keine konkrete Anleitung im Hinblick auf die zu setzenden Vorkehrungen gegeben, wenn abgefangenes Material an andere Parteien übermittelt wird. Es ist jedoch nun klar, dass einige Staaten regelmäßig Material mit ihren Geheimdienstpartnern teilen und diesen in manchen Fällen sogar direkten Zugang zu ihren eigenen Systemen gestatten. Folglich ist der GH der Ansicht, dass die Weitergabe von durch eine Massenüberwachung erlangtem Material durch einen Vertragsstaat an ausländische Staaten oder internationale Organisationen auf solches Material begrenzt werden sollte, das auf eine konventionskonforme Weise gesammelt und gespeichert wurde, und im Hinblick auf die Übermittlung selbst bestimmten weiteren Garantien unterworfen werden muss. Erstens müssen die Umstände, unter denen solch ein Transfer stattfinden darf, im innerstaatlichen Recht klar dargelegt werden. Zweitens muss der übermittelnde Staat sicherstellen, dass der empfangende Staat beim Umgang mit den Daten Garantien eingerichtet hat, die geeignet sind, Missbrauch und einen unverhältnismäßigen Eingriff zu verhindern. Insbesondere muss der empfangende Staat die sichere Aufbewahrung des Materials garantieren und seine weitere Offenlegung beschränken. Das bedeutet nicht notwendigerweise, dass der empfangende Staat einen vergleichbaren Schutz vorsehen muss wie der übermittelnde Staat. Auch wird dadurch nicht unbedingt verlangt, dass vor jedem Transfer eine Zusicherung abgegeben wird. Drittens werden verstärkte Garantien notwendig sein, wenn klar ist, dass Material, das eine besondere Vertraulichkeit verlangt – wie geheimes journalistisches Material – übermittelt wird. Letztlich befindet der GH, dass der Transfer von Material an ausländische Geheimdienstpartner auch einer unabhängigen Kontrolle unterliegen sollte.

(363) Aus den in Rn. 342 oben dargelegten Gründen ist der GH nicht überzeugt davon, dass die Erlangung von zugehörigen Kommunikationsdaten durch Massenüberwachung notwendigerweise weniger eingriffsintensiv ist als die Erlangung von Inhalten. Daher sollte die Überwachung, Speicherung und Durchsuchung von zugehörigen Kommunikationsdaten mit Bezugnahme auf dieselben Garantien analysiert werden wie jene, die im Hinblick auf den Inhalt anwendbar sind.

(364) Während die Überwachung von [...] Kommunikationsdaten normalerweise zur selben Zeit genehmigt werden wird wie die Überwachung von Inhalten, können sie nach Erlangung von den Geheimdiensten dennoch unterschiedlich behandelt werden. Angesichts des unterschiedlichen Charakters von [...] Kommunikationsdaten und der unterschiedlichen Arten, auf die sie von den Geheimdiensten verwendet werden, ist der GH, solange die vorgenannten Garantien eingerichtet sind, der Ansicht, dass die rechtlichen Bestimmungen, die ihre Behandlung regeln, nicht notwendig in jeder Hinsicht identisch mit jenen sein müssen, welche die Behandlung von Inhalten regeln.

c. Die Beurteilung des vorliegenden Falles

(366) [...] Der GH akzeptiert, dass das innerstaatliche Recht angemessen »zugänglich« war.

(367) Sich der Frage zuwendend, ob das Recht angemessene und wirksame Garantien enthielt, um die Anforderungen der »Vorhersehbarkeit« und »Notwendigkeit in einer demokratischen Gesellschaft« zu erfüllen, wird der GH jedes der acht in Rn. 361 dargelegten Erfordernisse im Hinblick auf die Überwachung von Inhalten von elektronischer Kommunikation (i) prüfen. Unter (ii) wird er genauer die Überwachung von zugehörigen Kommunikationsdaten prüfen.

▹

i. Überwachung von Kommunikationsinhalten

– die Gründe, aus denen eine Massenüberwachung genehmigt werden darf

(370) [...] Nach Ansicht des GH kann ein Regime, das es erlaubt, Massenüberwachung aus relativ weiten Gründen anzuordnen, dennoch mit Art. 8 EMRK in Einklang stehen, wenn insgesamt gesehen ausreichende Garantien gegen Missbrauch ins System eingebaut sind, um diesen Schwachpunkt zu kompensieren.

(371) Im Vereinigten Königreich konzentrierten sich die Gründe, aus denen Massenüberwachungen genehmigt werden konnten – obwohl sie relativ weit formuliert waren –, immer noch auf die nationale Sicherheit sowie schwere Verbrechen und das wirtschaftliche Wohl des Landes, soweit diese auch für die Interessen der nationalen Sicherheit relevant waren. [...]

– die Umstände, unter denen die Kommunikation eines Individuums überwacht werden darf

(376) [...] Unter dem Regime nach § 8 Abs. 4 RIPA konnte internationale Kommunikation (also solche, die über staatliche Grenzen hinweg erfolgte) überwacht werden. Die Geheimdienste verwendeten ihre Befugnis nur, um jene Übertragungsleitungen zu überwachen, die am wahrscheinlichsten grenzüberschreitende Kommunikation enthielten, an der ein geheimdienstliches Interesse bestand. Im Zusammenhang mit Massenüberwachung ist es schwierig, sich abstrakt vorzustellen, wie die Umstände, unter denen die Kommunikation eines Individuums überwacht werden kann, weiter begrenzt werden könnte. Da weder der Absender noch der Empfänger einer elektronischen Kommunikation den Übermittlungsweg zum Ziel kontrollieren konnte, hätten in der Praxis weitere Beschränkungen der Wahl der Übertragungsleitungen das innerstaatliche Recht im Hinblick auf seine Wirkungen jedenfalls nicht auf irgendeine Weise vorhersehbarer gemacht. Der GH akzeptiert daher, dass die Umstände, unter denen die Kommunikation eines Individuums unter dem Regime nach § 8 Abs. 4 RIPA überwacht werden konnte, ausreichend »vorhersehbar« iSd. Art. 8 EMRK waren.

– das für die Gewährung der Genehmigung einzuhaltende Verfahren

(383) [...] Das Fehlen irgendeiner Kontrolle der Kategorien von Selektoren zum Zeitpunkt der Genehmigung war ein Mangel [...]. Die nachträgliche Kontrolle der einzelnen Selektoren genügte [...] nicht. Auch wenn Analysten die Verwendung eines jeden Selektors im Hinblick auf die konventionsrechtlichen Grundsätze der Notwendigkeit und Verhältnismäßigkeit zu protokollieren und zu rechtfertigen hatten und diese Rechtfertigung einer unabhängigen Überwachung durch den ICC unterlag, waren starke Selektoren, die mit identifizierbaren Individuen in Zusammenhang stehen, dennoch keiner vorherigen internen Genehmigung unterworfen.

– die für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltenden Verfahren

(384) [...] Wenn eine Ermächtigung nach § 8 Abs. 4 RIPA zur Erlangung großer Mengen von Kommunikation führte, konnten dazu befugte Personen in der überwachenden Behörde starke Selektoren anwenden und komplexe Abfragen vornehmen, um einen Index zu generieren. Ein Selektor konnte sich dabei nicht auf ein Individuum beziehen, von dem bekannt war, dass es sich auf den Britischen Inseln aufhielt, und nicht die Identifikation von Material zum Ziel haben, das in Kommunikationen enthalten war, die von diesem Individuum selbst generiert worden oder für es bestimmt war. Etwas anderes galt nur, wenn der *Secretary of State* die Verwendung des Selektors persönlich genehmigt hatte, nachdem er sich zuerst davon überzeugt hatte, dass sie im Interesse der nationalen Sicherheit, zur Verhütung oder Aufspürung schwerer Verbrechen oder zum Schutz des wirtschaftlichen Wohles des Vereinigten Königreichs notwendig war, soweit diese Interessen auch für die Interessen der nationalen Sicherheit relevant waren, und sie verhältnismäßig war.

(385) Nur in dem Index enthaltenes Material konnte von einem Analysten geprüft werden und aufgrund irgendwelcher Kommunikationen oder Kommunikationsdaten konnte kein Geheimdienstbericht erstellt werden, wenn sie nicht zuvor durch einen Analysten geprüft worden waren. [...] Nur Material, auf das in der [der Ermächtigung beigeschlossenen] Bescheinigung durch den *Secretary of State* Bezug genommen wurde, stand einer menschlichen Überprüfung offen. Keinem Amtsträger war es gestattet, auf eine andere Weise Zugang zum Material zu erhalten als es die Bescheinigung vorsah. [...]

(386) [...] Obwohl die Bescheinigung bei der Regulierung des Zugangs zum abgefangenen Material eine wichtige Rolle spielte, [...] [wurde kritisiert], dass das in diesen Bescheinigungen bezeichnete Material sehr weit gefasst war. [...]

(387) Allerdings waren es [...] in der Praxis die Auswahl der Übertragungsleitungen, die Anwendung von einfachen Selektoren und anfänglichen Suchkriterien und dann komplexe Suchvorgänge, die bestimmten, welche Kommunikationen untersucht wurden. [...]

(388) [...] Ein Analyst, der Zugang zu Material im Index haben wollte, musste jeden Umstand angeben, der eine [...] Verletzung der Privatsphäre mit sich bringen konnte, zusammen mit den zur Reduktion des Ausmaßes dieses Eingriffs gesetzten Maßnahmen. Jeder folgende Zugang des Analysten war auf eine festgelegte Periode begrenzt. Wenn diese Periode verlängert wurde, musste das Protokoll mit Gründen für die Verlängerung aktualisiert werden [...]. [...] Es wurden regelmäßig Überprüfungen durchgeführt, die Checks einschlossen um sicherzustellen, dass die Protokolle betreffend die Anforderung von Zugang zu Material korrekt erstellt worden waren und dass das verlangte Material in die vom *Secretary of State* bestätigten Bereiche fiel.

(389) Zudem konnte [...] unter einer Ermächtigung nach § 8 Abs. 4 gesammeltes Material nur von einer befugten Person [...] gelesen, gesichtet oder angehört werden. Diese musste eine regelmäßige verpflichtende Ausbildung im Hinblick auf die Bestimmungen des RIPA und die Erfordernisse der Notwendigkeit und Verhältnismäßigkeit erhalten haben und angemessen überprüft worden sein. [...]

(390) [...] Abgefangenes Material konnte nur im für die autorisierten Zwecke notwendigen Ausmaß kopiert werden [...]. Jede Kopie [...] musste [...] auf eine sichere Weise aufbewahrt werden. [...]

(391) Vorbehaltlich der zuvor genannten Mängel bei der Genehmigung der Selektoren [...] und des allgemei-

nen Charakters der Bescheinigung des *Secretary of State* befindet der GH, dass die Umstände, unter denen abgefangenes Material unter dem Regime nach § 8 Abs. 4 ausgewählt, ausgewertet, verwendet und aufbewahrt werden konnte, iSd. Art. 8 EMRK ausreichend »vorhersehbar« waren und angemessene Garantien gegen Missbrauch boten.

– die zu treffenden Vorkehrungen, wenn das Material an andere Parteien übermittelt wird

(392) […] Folgendes war auf das für die »autorisierten Zwecke« notwendige Minimum zu beschränken: die Zahl der Personen, gegenüber denen das Material oder die Daten offengelegt oder verfügbar gemacht wurden; das Ausmaß, in dem das Material oder die Daten offengelegt oder verfügbar gemacht wurden; das Ausmaß, in dem das Material oder die Daten kopiert wurden; und die Anzahl der Kopien, die gemacht wurden. […] [Die innerstaatlichen Vorschriften führten näher aus, wann etwas für die autorisierten Zwecke »notwendig« war.]

(393) […] Die Offenlegung gegenüber Personen, die nicht ausreichend überprüft worden waren, war untersagt […] und abgefangenes Material konnte gegenüber einer Person nicht offengelegt werden, wenn die Aufgaben dieser Person, die mit einer der autorisierten Zwecke in Verbindung stehen mussten, nicht verlangten, dass sie im Hinblick auf das abgefangene Material »ein Informationsinteresse« besaß, um diese Aufgaben zu erfüllen. Gleichermaßen konnte abgefangenes Material nur in einem Umfang offengelegt werden, in dem es der Empfänger benötigte. […] Dies galt gleichermaßen für die Offenlegung gegenüber zusätzlichen Personen innerhalb einer Behörde wie für die Offenlegung nach außen. […]

(398) Es waren […] [auch] Garantien vorgesehen um zu gewährleisten, dass die Geheimdienstpartner für die sichere Aufbewahrung von übermitteltem Material sorgten und seine weitere Offenlegung beschränkten. Eine abschließende Garantie, der der GH besonderes Gewicht beimisst, ist die vom ICC und vom IPT gewährte Kontrolle.

(399) Im Lichte des Vorgesagten befindet der GH, dass die Vorkehrungen […] ausreichend klar waren und ausreichend robuste Garantien gegen Missbrauch boten.

– die Grenzen für die Dauer der Überwachung und der Aufbewahrung von abgefangenem Material und die Umstände, unter denen solches Material gelöscht und zerstört werden muss

(401) Angesichts der klaren Begrenzung der Dauer der Ermächtigungen nach § 8 Abs. 4 RIPA und des Erfordernisses, dass sie andauernd überprüft werden müssen, befindet der GH, dass die Regeln im Hinblick auf die Dauer von Überwachungen nach dem Regime des § 8 Abs. 4 ausreichend klar waren und angemessene Garantien gegen Missbrauch boten.

(402) […] Wenn ein Geheimdienst nicht analysiertes Überwachungsmaterial und zugehörige Kommunikationsdaten aufgrund einer Überwachung unter einer Ermächtigung nach § 8 Abs. 4 erhielt, hatte er Maximalspeicherperioden für unterschiedliche Kategorien von Material festzulegen, die die Natur und Eingriffsintensität widerspiegelten. Diese Perioden waren normalerweise nicht länger als zwei Jahre und mussten mit dem ICC abgesprochen werden. Soweit möglich, mussten alle Speicherperioden durch einen Prozess automatischer Löschung implementiert werden, der ausgelöst wurde, sobald die maximale Speicherfrist erreicht wurde. […] Gespeichertes Überwachungsmaterial musste in angemessenen Intervallen überprüft werden, um zu bestätigen, dass die Rechtfertigung für seine Aufbewahrung immer noch zutreffend […] war.

(403) […] Die Regierung brachte weitere Informationen zu den Speicherperioden vor. Kommunikationen, auf die lediglich das Verfahren der »starken Selektoren« angewendet wurde, wurden sofort gelöscht, wenn sie keine Übereinstimmung mit dem starken Selektor aufwiesen. Kommunikationen, auf die auch das »komplexe Abfrageverfahren« angewendet wurde, wurden für mehrere Tage gespeichert, damit das Verfahren durchgeführt werden konnte, und wurden dann automatisch gelöscht, wenn sie nicht für eine Auswertung ausgewählt wurden. Für eine Auswertung ausgewählte Kommunikationen konnten nur gespeichert werden, wenn dies notwendig und verhältnismäßig war. Standardmäßig war der Speicherzeitraum für ausgewählte Kommunikationen nicht länger als einige Monate – dann wurden sie automatisch gelöscht […]. In außergewöhnlichen Fällen konnte jedoch vertreten werden, ausgewählte Kommunikationen für längere Zeit zu speichern. In der Praxis waren die Speicherzeiträume daher offenbar wesentlich kürzer als die zweijährige Maximumfrist.

(404) Schließlich musste […] jede Kopie von Überwachungsmaterial […] zerstört werden, sobald die Speicherung nicht länger notwendig war […].

(405) […] Das IPT prüfte die Vorkehrungen für die Speicherung von Material und seine Zerstörung und erachtete sie für angemessen. Der GH hält die […] Vorkehrungen […] auch für ausreichend klar. Seiner Ansicht nach wäre es jedoch wünschenswert gewesen, dass sich die kürzeren Speicherzeiträume, die von der Regierung im Laufe des vorliegenden Verfahrens bezeichnet wurden, in den geeigneten legislativen und/oder anderen allgemeingültigen Maßnahmen widergespiegelt hätten.

– Kontrolle

(412) Der GH ist überzeugt davon, dass der ICC eine unabhängige und wirksame Kontrolle des Betriebs des Regimes nach § 8 Abs. 4 bot. Insbesondere konnte er […] die Notwendigkeit und Verhältnismäßigkeit einer bedeu-

tenden Zahl von [...] Ermächtigungen und die folgende Wahl von Selektoren beurteilen und das für die Speicherung, Aufbewahrung und Zerstörung abgefangener Kommunikation und zugehöriger Kommunikationsdaten vorgesehene Verfahren untersuchen. Er konnte auch gegenüber den Leitern der betroffenen Behörden Empfehlungen aussprechen. Diese Behörden mussten binnen zwei Monaten über die Fortschritte berichten, die sie im Hinblick auf die Umsetzung dieser Empfehlungen gemacht hatten. Zudem bestätigte die Regierung [...], dass der ICC vom GCHQ regelmäßig über die Basis informiert wurde, auf welcher Übertragungsleitungen für eine Überwachung ausgewählt wurden. Die Geheimdienste waren verpflichtet, in jeder Phase des Massenüberwachungsverfahrens Aufzeichnungen zu führen und Prüfern Zugang zu diesen Aufzeichnungen zu gewähren. Schließlich überwachte er auch die Weitergabe von Überwachungsmaterial an Geheimdienstpartner.

– *ex post facto*-Überprüfung

(413) Eine *ex post facto*-Überprüfung wurde vom IPT geboten, dem im vorliegenden Fall jedes Mal ein Richter des *High Court* vorsaß. Die Kammer stellte fest [...], dass das IPT einen wirksamen Rechtsbehelf für Bf. bietet, die sich über spezielle Vorfälle von Überwachungen oder die allgemeine Konventionskonformität beschweren. Sie erachtete es für bedeutsam, dass das IPT umfassende Jurisdiktion hatte, um jede Beschwerde wegen einer unrechtmäßigen Überwachung zu untersuchen, die nicht von der Benachrichtigung einer Zielperson abhing. Daher konnte jede Person, die glaubte, geheimer Überwachung unterworfen worden zu sein, eine Beschwerde an es richten. Seine Mitglieder mussten ein hohes Richteramt innegehabt haben oder qualifizierte Anwälte sein, die zumindest zehn Jahre praktiziert hatten. Die an der Genehmigung und Vollstreckung einer Überwachungsermächtigung Beteiligten waren verpflichtet, dem IPT alle benötigten Dokumente offenzulegen, einschließlich [...] solcher, die aus Gründen der nationalen Sicherheit nicht öffentlich gemacht werden konnten. Ferner hatte es ein Ermessen, mündliche und wenn möglich öffentliche Verhandlungen abzuhalten [...]. Wenn es über eine Beschwerde entschied, hatte es die Befugnis, eine Entschädigung zuzusprechen und jede andere Anordnung zu erteilen, die es für geeignet hielt, einschließlich der Aufhebung oder des Widerrufs einer Ermächtigung oder der Zerstörung der Aufzeichnungen. Schließlich wurden seine rechtlichen Entscheidungen auf seiner eigenen Webseite veröffentlicht [...].

(414) Zudem war das IPT zuständig, jede Beschwerde hinsichtlich der Konventionskonformität der Weitergabe von Überwachungsmaterial an Dritte oder hinsichtlich des Regimes über die Weitergabe von Überwachungsmaterial zu prüfen. [...]

(415) Der GH ist daher überzeugt davon, dass das IPT jedem ein robustes Rechtsmittel bot, der den Verdacht hatte, dass seine Kommunikation von den Geheimdiensten überwacht worden war.

ii. Kommunikationsdaten

(416) [...] Ermächtigungen nach § 8 Abs. 4 genehmigten die Überwachung von Inhalts- und zugehörigen Kommunikationsdaten. Letztere wurden unter dem Regime des § 8 Abs. 4 größtenteils gleichbehandelt. Daher betreffen die Mängel, die im Hinblick auf dieses Regime bereits im Zusammenhang mit der Überwachung von Inhalten festgestellt wurden [...], gleichermaßen die zugehörigen Kommunikationsdaten [...].

(417) Gleichzeitig profitierte die Behandlung von Kommunikationsdaten zum größten Teil von denselben Garantien wie der Inhalt. [...]

(419) Es gab jedoch zwei wesentliche Bereiche, in denen das Regime zur Massenüberwachung Inhalt und zugehörige Kommunikationsdaten verschieden behandelte: Letztere waren von der Garantie nach § 16 Abs. 2 RIPA ausgeschlossen. Das bedeutete, dass ein Analyst, wenn er einen Selektor verwenden wollte, der sich auf ein Individuum bezog, von dem bekannt war, dass es sich zur Zeit auf den Britischen Inseln befand, nicht verpflichtet war, die Verwendung dieses Selektors vom *Secretary of State* als notwendig und verhältnismäßig bestätigen zu lassen. [...] Kommunikationsdaten, bei denen es weder durch den Einsatz eines starken Selektors noch durch eine komplexe Datenabfrage zu einer Übereinstimmung gekommen war, wurden nicht sofort zerstört, sondern stattdessen für eine Maximalperiode von bis zu mehreren Monaten gespeichert. Der GH wird daher prüfen, ob das innerstaatliche Recht das im Zusammenhang mit der Auswahl der [...] Kommunikationsdaten zur Auswertung einzuhaltende Verfahren sowie die Grenzen der Dauer der Speicherung solcher Daten klar definierte.

(421) Der GH akzeptiert, dass [...] Kommunikationsdaten im Kampf gegen Terrorismus und schweres Verbrechen ein wesentliches Werkzeug für die Geheimdienste sind und es Umstände geben kann, unter denen es notwendig und verhältnismäßig ist, nach solchen Daten von Personen, die sich bekanntermaßen im Vereinigten Königreich aufhalten, zu suchen und darauf zuzugreifen. Während § 16 Abs. 2 zudem eine wichtige Garantie im Zusammenhang mit dem Verfahren zur Auswahl von Überwachungsmaterial zur Auswertung umfasst, ist hervorzuheben, dass der GH bei der Beurteilung des Regimes der Massenüberwachung von Inhalten wesentlich mehr Gewicht auf die Existenz eines wirksamen Mechanismus legte um sicherzustellen, dass die Auswahl von Selektoren den konventionsrechtlichen Anforderungen der Notwendigkeit und Verhältnismäßigkeit sowie interner und externer Kontrolle unterworfen war. Wenn der GH daher die Bedenken wiederholt, die im

Hinblick auf die Auswahl und Kontrolle von Selektoren […] [im Zusammenhang mit den Inhalten] aufgeworfen wurden, befindet er doch nicht, dass der Ausschluss zugehöriger Kommunikationsdaten von der Garantie nach § 16 Abs. 2 bei der Gesamtbeurteilung entscheidendes Gewicht haben sollte.

(422) Was die Dauer der Speicherung angeht, behauptete die Regierung, dass zugehörige Kommunikationsdaten »mehr analytische Arbeit über einen längeren Zeitraum verlangen […]«. Dies […] könne die Auswertung von Elementen einschließen, die ursprünglich nicht von geheimdienstlichem Interesse gewesen waren. Die sofortige Löschung von nicht ausgewählten Kommunikationsdaten oder eine Löschung nach ein paar Tagen würde dies unmöglich machen.

(423) Angesichts des Vorgesagten, der Existenz einer Maximalspeicherfrist, die »mehrere Monate« nicht überstieg, und des Umstands, dass die Ungleichbehandlung objektiv und angemessen gerechtfertigt war, akzeptiert der GH, dass die Vorschriften zur Speicherung von […] Kommunikationsdaten ausreichend […] waren, auch wenn sie sich von den Vorschriften betreffend Inhalte wesentlich unterschieden. Allerdings wurden diese Speicherzeiträume erst im Verfahren vor dem GH offengelegt. Folglich waren diese kürzeren Fristen für jemanden, der den *Interception of Communications Code of Practice* (»*IC Code*«) las, nicht ersichtlich. Es gab auch keinen Hinweis in selbigem, dass die Speicherzeiträume für […] Kommunikationsdaten sich von jenen für Inhalte unterschieden. Nach Ansicht des GH sollten die im Verfahren vor ihm enthüllten Speicherperioden in geeignete legislative und/oder andere allgemeingültige Maßnahmen aufgenommen werden, um die aus Art. 8 EMRK erfließenden Anforderungen an die »Vorhersehbarkeit« zu erfüllen.

iii. Ergebnis

(424) Der GH akzeptiert, dass Massenüberwachung für die Vertragsstaaten große Bedeutung hat, um Bedrohungen für ihre nationale Sicherheit zu identifizieren. […] Der *Independent Reviewer of Terrorism Legislation*[2] […] kam zum Schluss, dass sie ein wesentliches Potential hat: erstens, weil Terroristen, Verbrecher und feindliche ausländische Geheimdienste zunehmend geschickt darin geworden wären, der Entdeckung durch traditionelle Mittel zu entkommen; und zweitens, weil das globale Internet bewirken würde, dass der Weg, den eine spezielle Kommunikation nimmt, höchst unvorhersehbar geworden ist. Obwohl er und sein Team Alternativen zur Massenüberwachung erwogen […], kamen sie zum Schluss, dass keine Alternative oder Kombination von Alternativen ausreichte, um die Durchschlagskraft der Massenüberwachung zu ersetzen.

(425) Dennoch erinnert der GH daran, dass Massenüberwachung ein beträchtliches Potential aufweist, auf eine Weise missbraucht zu werden, welche die Rechte von Individuen auf Achtung ihres Privatlebens beeinträchtigt. […] Das Regime nach § 8 Abs. 4 umfasste insgesamt gesehen […] keine ausreichenden »durchgehenden Garantien«, um angemessen und wirksam gegen Willkür und die Gefahr von Missbrauch zu schützen. Insbesondere hat der GH die folgenden grundlegenden Mängel identifizert: das Fehlen einer unabhängigen Genehmigung, das Versäumnis, die Kategorien von Selektoren in den Antrag auf eine Ermächtigung aufzunehmen, und das Versäumnis, Selektoren, die mit einem Individuum verbunden sind, einer vorherigen internen Genehmigung zu unterwerfen […]. Diese Schwachpunkte betrafen nicht nur die Überwachung von Inhalten von Kommunikationen, sondern auch jene von zugehörigen Kommunikationsdaten. Auch wenn der ICC eine unabhängige und wirksame Kontrolle des Regimes bot, und das IPT jedem, der den Verdacht hegte, dass seine Kommunikation von den Geheimdiensten abgehört worden war, ein starkes gerichtliches Rechtsmittel bot, waren diese Garantien nicht ausreichend, um die Mängel […] zu kompensieren.

(426) Angesichts der oben genannten Mängel befindet der GH, dass § 8 Abs. 4 die Anforderungen an die »Qualität des Gesetzes« nicht erfüllte und daher nicht geeignet war, den »Eingriff« auf das zu beschränken, was »in einer demokratischen Gesellschaft notwendig« war.

(427) Es erfolgte daher eine **Verletzung** von **Art. 8 EMRK** (einstimmig; *im Ergebnis übereinstimmendes gemeinsames Sondervotum der Richter Lemmens, Vehabović and Bošnjak; im Ergebnis übereinstimmendes Sondervotum von Richter Pinto de Albuquerque*).

2. Zur behaupteten Verletzung von Art. 10 EMRK

(428) Die bf. [Journalisten] […] brachten vor, dass der von Art. 10 EMRK […] gewährte Schutz [für ihre Tätigkeit] von wesentlicher Bedeutung war. […]

a. Der im vorliegenden Fall zu verfolgende Ansatz

(447) Unter dem Regime nach § 8 Abs. 4 konnte vom Geheimdienst auf vertrauliches journalistisches Material entweder gezielt zugegriffen werden – durch den bewussten Einsatz von Selektoren oder Suchbegriffen, die mit einem Journalisten oder einer Nachrichtenorganisation verbunden waren – oder unabsichtlich als »Beifang« der Operation zur Massenüberwachung.

(448) Wenn es die Absicht der Geheimdienste ist, z.B. durch den bewussten Einsatz von starken Selektoren, die einen Zusammenhang zu einem Journalisten

2 Bei diesem handelt es sich um eine von der Regierung unabhängige Person, die damit betraut ist, dem Innenminister und Parlament über die Umsetzung der Antiterrorgesetze im Vereinigten Königreich zu berichten.

aufweisen, auf vertrauliches journalistisches Material zuzugreifen, oder wenn als Folge der Auswahl solcher starker Selektoren eine hohe Wahrscheinlichkeit besteht, dass solches Material für die Auswertung ausgewählt wird, ist der Eingriff vergleichbar mit jenem, der durch die Durchsuchung der Wohnung oder des Arbeitsplatzes eines Journalisten verursacht wird. Unabhängig davon, ob es die Absicht der Geheimdienste ist, eine Quelle zu identifizieren, würde die Verwendung von Selektoren oder Suchbegriffen, die mit einem Journalisten in Zusammenhang stehen, sehr wahrscheinlich zur Erlangung von bedeutenden Mengen vertraulichen journalistischen Materials führen, die den Schutz von Quellen sogar zu einem größeren Ausmaß unterlaufen könnte als eine Anordnung zur Offenlegung einer Quelle. Daher befindet der GH, dass – bevor die Geheimdienste entsprechende Selektoren oder Suchbegriffe verwenden – diese von einem Richter oder einem sonstigen unabhängigen und unparteiischen Entscheidungsorgan genehmigt worden sein müssen, die mit der Befugnis ausgestattet sind zu entscheiden, ob sie »durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt« sind und insbesondere ob eine weniger eingreifende Maßnahme ausreichen würde, um dem vorrangigen öffentlichen Interesse zu genügen.

(449) Selbst wenn keine Absicht besteht, auf vertrauliches journalistisches Material zuzugreifen, und die verwendeten Selektoren und Suchbegriffe die Auswahl von vertraulichem journalistischem Material zur Auswertung nicht sehr wahrscheinlich machen, besteht dennoch eine Gefahr, dass solches Material als »Beifang« einer Operation zur Massenüberwachung abgefangen und sogar ausgewertet wird. Nach Ansicht des GH unterscheidet sich diese Situation wesentlich von der gezielten Überwachung eines Journalisten […]. Da die Überwachung von journalistischen Kommunikationen hier unabsichtlich ist, kann das Ausmaß des Eingriffs in diese und/oder journalistische Quellen nicht vorhergesehen werden. Folglich wäre es im Stadium der Genehmigung für einen Richter oder ein sonstiges unabhängiges Organ nicht möglich zu beurteilen, ob ein solcher Eingriff »durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt« wäre und insbesondere ob eine weniger eingreifende Maßnahme ausgereicht hätte, um dem vorrangigen öffentlichen Interesse zu genügen.

(450) Im Fall *Weber und Saravia/D* hielt der GH fest, dass der Eingriff in die Meinungsäußerungsfreiheit durch »strategische Überwachung« nicht als besonders schwerwiegend eingestuft werden konnte, da er nicht darauf abzielte, Journalisten zu überwachen und die Behörden – wenn überhaupt – erst, wenn sie die abgefangenen Telekommunikationen auswerteten, erkennen konnten, dass die Kommunikation eines Journalisten überwacht wurde. Daher akzeptierte er, dass die anfängliche Überwachung ohne Auswertung des abgefangenen Materials keinen schwerwiegenden Eingriff in Art. 10 EMRK darstellte. Dennoch hat der GH bereits festgehalten, dass im gegenwärtigen, zunehmend digitalen Zeitalter die technischen Möglichkeiten das Volumen an Kommunikationen, die das globale Internet durchlaufen, stark gesteigert haben und als Folge davon Überwachungen, die nicht direkt auf Individuen abzielen, in der Tat eine sehr große Reichweite haben können, und zwar sowohl innerhalb als auch außerhalb des Gebiets des überwachenden Staates. Da die Auswertung der Kommunikationen eines Journalisten oder zugehöriger Kommunikationsdaten durch einen Analysten zur Identifikation einer Quelle führen könnte, erachtet es der GH für unabdingbar, dass das innerstaatliche Recht robuste Garantien im Hinblick auf die Aufbewahrung, Auswertung, Verwendung, Weitergabe und Zerstörung solchen vertraulichen Materials umfasst. Selbst wenn eine journalistische Kommunikation oder zugehörige Kommunikationsdaten nicht durch die bewusste Verwendung eines Selektors oder Suchbegriffs, von dem bekannt war, dass er mit einem Journalisten in Zusammenhang stand, zur Auswertung ausgewählt wurden, darf – wenn offensichtlich wird, dass die Kommunikation oder zugehörige Kommunikationsdaten vertrauliches journalistisches Material enthalten – ihre weitere Aufbewahrung und Auswertung durch einen Analysten nur möglich sein, wenn dies durch einen Richter oder ein sonstiges unabhängiges und unparteiisches Entscheidungsorgan genehmigt wurde, die mit der Befugnis ausgestattet sind zu entscheiden, ob eine weitere Aufbewahrung und Auswertung »durch ein vorrangiges Erfordernis im öffentlichen Interesse gerechtfertigt« ist.

b. Anwendung des Tests auf den vorliegenden Fall

(451) […] Da es sich bei den Bf. des zweiten Falles um eine Nachrichtenorganisation und einen Journalisten handelt, akzeptiert der GH, dass das Regime nach § 8 Abs. 4 auch in ihre Rechte nach Art. 10 EMRK […] eingriff.

(453) […] Im *IC Code* waren einige zusätzliche Garantien für vertrauliches journalistisches Material vorgesehen.

(456) […] Der GH akzeptiert, dass die Garantien im *IC Code* betreffend die Aufbewahrung, Weitergabe und Zerstörung von vertraulichem journalistischem Material angemessen waren. Die zusätzlichen Garantien im *IC Code* sprachen jedoch nicht die Schwachpunkte an, die der GH bei seiner Analyse des Regimes unter Art. 8 EMRK feststellte, und sie erfüllten auch nicht die vom GH in den Rn. 448-450 bezeichneten Anforderungen. Insbesondere existierte kein Erfordernis, dass die Verwendung von Selektoren oder Suchbegriffen, von denen bekannt war, dass sie mit einem Journalisten in Zusam-

menhang standen, durch einen Richter oder ein sonstiges unabhängiges und unparteiisches Entscheidungsorgan genehmigt wurde [...]. Wenn eine Absicht bestand, auf vertrauliches journalistisches Material zuzugreifen, oder dies angesichts der Verwendung von Selektoren, die in Zusammenhang mit einem Journalisten standen, sehr wahrscheinlich war, war ganz im Gegenteil lediglich verlangt, dass die Gründe sowie die Notwendigkeit und Verhältnismäßigkeit dafür eindeutig dokumentiert wurden.

(457) Zudem waren unzureichende Garantien vorgesehen um sicherzustellen, dass wenn es offensichtlich wurde, dass eine Kommunikation, die nicht durch die bewusste Verwendung eines entsprechenden Selektors oder Suchbegriffs [...] zur Auswertung ausgewählt wurde, trotzdem vertrauliches journalistisches Material umfasste, diese nur weiter aufbewahrt und von einem Analysten ausgewertet werden konnte, wenn dies von einem Richter oder einem sonstigen unabhängigen und unparteiischen Entscheidungsorgan genehmigt worden war [...]. Stattdessen wurde [...] lediglich verlangt, dass einer Überwachung, die vertrauliches journalistisches Material umfassen konnte, »besondere Beachtung« geschenkt wurde.

(458) Angesichts dieses Schwachpunktes und der vom GH im Zusammenhang mit der Prüfung der Beschwerde unter Art. 8 EMRK identifizierten Mängel stellt er fest, dass [...] eine **Verletzung** von **Art. 10 EMRK** erfolgt ist (einstimmig; *im Ergebnis übereinstimmendes gemeinsames Sondervotum der Richter Lemmens, Vehabović and Bošnjak; im Ergebnis übereinstimmendes Sondervotum von Richter Pinto de Albuquerque*).

▷

III. Zum Erhalt von Informationen durch ausländische Geheimdienste gemäß Kapitel 12 des *IC Codes*

1. Zur behaupteten Verletzung von Art. 8 EMRK

(462) Die GK wird ihre Untersuchung auf die Beschwerde wegen des Erhalts von angefordertem Überwachungsmaterial von der NSA beschränken.

a. Zum anwendbaren Test

(495) Nach Ansicht der Kammer konnte die Überwachung von Kommunikationen durch ausländische Geheimdienste nicht die Verantwortlichkeit eines Empfangsstaates auf den Plan rufen oder in dessen Hoheitsgewalt iSd. Art. 1 EMRK fallen, auch wenn die Überwachung auf dessen Ersuchen hin vorgenommen wurde. [...]

(496) Die GK stimmt der Kammer zu [...]. Daher konnte ein Eingriff in Art. 8 EMRK nur im anfänglichen Ersuchen um Überwachungsmaterial und dessen folgendem Erhalt bestehen, an den sich dessen Aufbewahrung, Auswertung und Verwendung durch die Geheimdienste des Empfangsstaates schloss.

(497) Der von der Konvention gewährte Schutz würde belanglos, wenn die Staaten ihre Konventionsverpflichtungen umgehen könnten, indem sie entweder die Überwachung von Kommunikation durch Nichtvertragsstaaten oder die Übermittlung abgefangener Kommunikation durch diese verlangen oder indem sie – auch wenn dies in den vorliegenden Fällen nicht direkt in Frage steht – solche Kommunikation direkt durch Zugang zu deren staatlichen Datenbanken erhalten. Wenn daher ein Nichtvertragsstaat um Überwachungsmaterial ersucht wird, muss dafür [...] eine Grundlage im innerstaatlichen Recht existieren, die für die betroffene Person zugänglich und im Hinblick auf ihre Konsequenzen vorhersehbar sein muss. Es ist auch notwendig, klare und detaillierte Regeln zu haben, die Bürgern einen angemessenen Hinweis auf die Umstände und Bedingungen geben, unter denen die Behörden befugt sind, ein solches Ersuchen zu stellen, und die wirksame Garantien gegen die Verwendung dieser Befugnis bieten, um das innerstaatliche Recht und/oder die Verpflichtungen des Staates unter der Konvention zu umgehen.

(498) Bei Erhalt des abgefangenen Materials muss der empfangende Staat angemessene Garantien für die Auswertung, Verwendung, Aufbewahrung, Weitergabe sowie Löschung und Zerstörung vorsehen. Diese Garantien, die vom GH zunächst in seiner Rechtsprechung zur Überwachung von Kommunikation durch Vertragsstaaten entwickelt wurden, sind gleichermaßen auf den Erhalt von erbetenem Überwachungsmaterial von einem ausländischen Geheimdienst durch einen Vertragsstaat anwendbar. Zur Behauptung der Regierung, die Staaten würden nicht immer wissen, ob Material, das sie von ausländischen Geheimdiensten erhalten, das Produkt einer Überwachung ist, befindet der GH, dass dieselben Standards auf jedes Material anzuwenden sind, das von ausländischen Geheimdiensten erlangt wird und das das Produkt von Überwachung sein könnte.

(499) Schließlich befindet der GH, dass jedes Regime, das es den Geheimdiensten erlaubt, von Nichtvertragsstaaten eine Überwachung oder Überwachungsmaterial oder direkten Zugang zu solchem Material zu verlangen, einer unabhängigen Kontrolle unterworfen werden und auch die Möglichkeit einer *ex post facto*-Überprüfung bestehen sollte.

b. Anwendung des Tests auf den vorliegenden Fall

(501) [...] Das Regime betreffend das Ersuchen um Infor-

mationen von Nichtvertragsstaaten und deren Erhalt hatte eine klare Grundlage im innerstaatlichen Recht, die […] angemessen zugänglich war. Da es ohne Zweifel die legitimen Ziele des Schutzes der nationalen Sicherheit, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer verfolgte, wird der GH […] die Vorhersehbarkeit und Notwendigkeit des Regimes beurteilen.

(502) Kapitel 12 des *IC Code* folgt demselben Ansatz wie die innerstaatliche Gesetzgebung zu Massenüberwachung. Die Geheimdienste konnten ein Ersuchen an eine ausländische Regierung im Hinblick auf nicht analysierte abgefangene Kommunikationen und/oder Kommunikationsdaten nur stellen, wenn vom *Secretary of State* bereits eine einschlägige Überwachungsermächtigung unter dem RIPA erteilt worden war, die Hilfe der ausländischen Regierung notwendig war, um die speziellen Kommunikationen zu bekommen, weil sie unter der bestehenden Ermächtigung nicht erlangt werden konnten […], und es für die überwachende Behörde notwendig und verhältnismäßig war, diese Kommunikationen zu erlangen.

(503) Unter außergewöhnlichen Umständen konnte ein Ersuchen um Kommunikationen ohne eine einschlägige Überwachungsermächtigung nach dem RIPA gestellt werden […]. […] [Laut der Regierung] wurde [davon allerdings in der Praxis] noch nie […] [Gebrauch gemacht].

(506) Da die innerstaatliche Gesetzgebung im Hinblick auf Ersuchen um Informationsaustausch demselben Ansatz folgte wie Massenüberwachung und das nationale Recht explizit vorsah, dass es keine Umgehung geben dürfe, besteht für den GH keine Notwendigkeit, das Genehmigungsverfahren gesondert zu betrachten.

(507) Was die Garantien für die Auswertung, Verwendung, Aufbewahrung, Weitergabe, Löschung und Zerstörung des erbetenen Überwachungsmaterials angeht, war […] klar, dass abgefangene Inhalte oder zugehörige Kommunikationsdaten, die von den Geheimdiensten des Vereinigten Königreichs von einem anderen Staat erlangt worden waren und sich als Produkt einer Überwachung darstellen, denselben innerstaatlichen Regeln und Garantien unterworfen werden mussten, die auf dieselben Kategorien von Inhalten oder Daten Anwendung fanden, wenn diese von den überwachenden Behörden als Folge einer Überwachung nach dem RIPA direkt erlangt wurden. […]

(508) Der GH hat die Garantien im Hinblick auf das Regime der Massenüberwachung untersucht und war überzeugt, dass die Verfahren […] ausreichend klar waren und angemessenen Schutz gegen Missbrauch gewährten (siehe Rn. 384-405 oben). […] Der GH bemerkt, dass […] die Garantien […] nicht auf jedes Material erstreckt wurden, das von ausländischen Geheimdiensten erlangt wurde und Produkt einer Überwachung sein konnte. Diese Garantien waren auf Material beschränkt, dass sich als solches darstellte. Dieser Umstand alleine machte das Regime jedoch nicht mit Art. 8 EMRK unvereinbar.

(509) Im Zusammenhang mit dem Regime nach § 8 Abs. 4 hatte der GH Bedenken im Hinblick auf die Ausnahme von […] Kommunikationsdaten von der Garantie nach § 16 RIPA. […] Unter Kapitel 12 des *IC Code* wurden Inhalte und […] Kommunikationsdaten […] [jedoch] von den Geheimdiensten nicht massenweise verlangt. § 12.5 […] wies darauf hin, dass ein Ersuchen, wenn es auf eine bestehende Ermächtigung gestützt wurde, mit Bezug auf konkrete Selektoren (also konkrete Individuen) gestellt wurde, und der *Secretary of State* das Ersuchen um Kommunikationen von diesen Individuen bereits genehmigt hatte. […]

(513) Daher befindet der GH, dass das Regime betreffend das Ersuchen um abgefangenes Material und dessen Erhalt mit Art. 8 EMRK vereinbar war. Es existierten klare und detaillierte Regeln, die den Bürgern einen angemessenen Hinweis auf die Umstände und Bedingungen gaben, unter denen die Behörden befugt waren, ein Ersuchen an einen ausländischen Geheimdienst zu stellen; das nationale Recht umfasste wirksame Garantien gegen die Verwendung solcher Ersuchen, um das innerstaatliche Recht und/oder die Verpflichtungen des Vereinigten Königreichs unter der Konvention zu umgehen; Letzteres hatte angemessene Garantien für die Auswertung, Verwendung, Aufbewahrung, Weitergabe, Löschung und Zerstörung des Materials eingerichtet; und das Regime wurde einer unabhängigen Kontrolle durch den ICC unterworfen und es gab eine Möglichkeit für eine *ex post facto*-Überprüfung durch das IPT.

(514) Folglich kam es zu **keiner Verletzung** von **Art. 8 EMRK** (12:5 Stimmen; *gemeinsames abweichendes Sondervotum der Richter Lemmens, Vehabović, Ranzoni und Bošnjak; abweichendes Sondervotum von Richter Pinto de Albuquerque*).

2. Zur behaupteten Verletzung von Art. 10 EMRK

(516) Die Bf. des dritten Falles behaupteten […] die Unvereinbarkeit des Informationsaustauschregimes mit Art. 10 EMRK. […] Der GH stimmt der Kammer zu, dass diese Rüge keine Frage aufwirft, die über jene unter Art. 8 EMRK hinausgeht. Er befindet daher, dass auch **keine Verletzung** von **Art. 10 EMRK** erfolgt ist (12:5 Stimmen; *gemeinsames abweichendes Sondervotum der Richter Lemmens, Vehabović, Ranzoni and Bošnjak; abweichendes Sondervotum von Richter Pinto de Albuquerque*).

IV. Erlangung von Kommunikationsdaten von Kommunikationsdienstleistern nach Kapitel II des RIPA

[Die Bf. des zweiten Falles rügten, das Regime für die Erlangung von Kommunikationsdaten von Kommunikationsdienstleistern unter Kapitel II des RIPA wäre nicht mit ihren Rechten unter Art. 8 und Art. 10 EMRK vereinbar.]

1. Zur behaupteten Verletzung von Art. 8 EMRK

(518) Zum Zeitpunkt der Untersuchung des Falles durch die Kammer war die Regierung des Vereinigten Königreichs gerade dabei, den bestehenden rechtlichen Rahmen für die Durchführung geheimer Überwachungen durch das neue IPA zu ersetzen. Die Bestimmungen der neuen Gesetzgebung zur Speicherung von Kommunikationsdaten durch Kommunikationsdienstleister waren Gegenstand einer innerstaatlichen gerichtlichen Anfechtung […]. Im Laufe dieses Verfahrens gestand die Regierung ein, dass die einschlägigen Bestimmungen nicht mit den Anforderungen aus dem EU-Recht in Einklang standen. Folglich stellte der *High Court* fest, dass Teil 4 des IPA nicht mit den EU-Grundrechten vereinbar war, da der Zugang zu gespeicherten Daten im Bereich der Strafjustiz nicht auf den Zweck der Bekämpfung »schwerer Verbrechen« beschränkt war und keiner vorherigen Überprüfung durch ein Gericht oder ein unabhängiges Verwaltungsorgan unterlag.

(519) […] Da das frühere Regime an denselben »Mängeln« gelitten hatte wie sein Nachfolger, stellte die Kammer fest, dass es nicht »gesetzlich vorgesehen« iSd. Art. 8 EMRK war.

(522) Deshalb befindet der GH, dass im vorliegenden Fall eine **Verletzung** von **Art. 8 EMRK** erfolgte […] (einstimmig; *im Ergebnis übereinstimmendes gemeinsames Sondervotum der Richter Lemmens, Vehabović und Bošnjak; im Ergebnis übereinstimmendes Sondervotum von Richter Pinto de Albuquerque*).

▷

2. Zur behaupteten Verletzung von Art. 10 EMRK

(524) Die Kammer anerkannte, dass das Regime nach Kapitel II einen verstärkten Schutz bot, wenn um Daten ersucht wurde, um eine journalistische Quelle zu identifizieren. […]

(525) Diese Bestimmungen fanden jedoch nur Anwendung, wenn der Zweck des Antrags darin lag, eine Quelle zu bestimmen. Sie waren nicht in jedem Fall anwendbar, in dem um die Kommunikationsdaten eines Journalisten ersucht wurde oder in dem ein solcher kollateraler Eingriff wahrscheinlich war. Zudem gab es für Fälle betreffend den Zugang zu Kommunikationsdaten eines Journalisten keine speziellen Bestimmungen, die den Zugang auf den Zweck der Bekämpfung »schwerer Verbrechen« beschränkte. Daher befand die Kammer, dass das Regime nicht »gesetzlich vorgesehen« iSd. Art. 10 EMRK […] war.

(528) Folglich befindet der GH, dass im vorliegenden Fall eine **Verletzung** von **Art. 10 EMRK** erfolgte […] (einstimmig; *im Ergebnis übereinstimmendes gemeinsames Sondervotum der Richter Lemmens, Vehabović and Bošnjak; im Ergebnis übereinstimmendes Sondervotum von Richter Pinto de Albuquerque*).

V. Entschädigung nach Art. 41 EMRK

Die Bf. beantragten keine Entschädigung für erlittenen Schaden. € 227.500,– an die Bf. des ersten Falls, € 90.000,– an die Bf. des zweiten Falls und € 36.000,– an die Bf. des dritten Falls für Kosten und Auslagen (einstimmig).