FAMOS
Der **Fa**ll des **Mo**nats im **S**trafrecht

Humboldt-Universität zu Berlin · Juristische Fakultät · Professur für Strafrecht, Strafprozessrecht und Rechtsphilosophie
Prof. Dr. Klaus Marxen sowie Mitarbeiterinnen und Mitarbeiter der Professur und Studierende

04
2006

April 2006

Verbindungsdaten-Fall

Sicherstellung von gespeicherten Telekommunikationsdaten im Herrschaftsbereich des Teilnehmers / verfassungsrechtliche Anforderungen an Durchsuchung und Beschlagnahme zum Zweck der Datensicherstellung / Verhältnismäßigkeit

§§ 94 ff., 102 ff. StPO, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, 10, 13 GG

Leitsätze des Gerichts (Auszug): Die nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten werden nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) geschützt. §§ 94 ff. und §§ 102 ff. StPO genügen den verfassungsrechtlichen Anforderungen auch hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten. Beim Zugriff auf die bei dem Betroffenen gespeicherten Verbindungsdaten ist auf deren erhöhte Schutzwürdigkeit Rücksicht zu nehmen.

BVerfG, Urteil vom 2. März 2006 – Az 2 BvR 2099/04; veröffentlicht in NJW 2006, 976

1. Sachverhalt[1]

Richterin A gerät in den Verdacht, Informationen aus einem Ermittlungsverfahren wegen terroristischer Straftaten an einen befreundeten Journalisten weitergegeben zu haben, der über das Verfahren berichtet hat. Gegen sie wird ein Ermittlungsverfahren wegen des Verdachts der Verletzung von Dienstgeheimnissen eingeleitet. Nach etwa fünf Monaten ordnet das Landgericht auf Antrag der Staatsanwaltschaft die Durchsuchung der Wohnung und des Dienstzimmers der A und die Beschlagnahme ihrer Computer und ihres Mobiltelefons an. Die Maßnahme hat zum Ziel, durch Sicherstellung von gespeicherten Verbindungsdaten den Nachweis zu ermöglichen, dass A im zeitlichen Zusammenhang mit der Veröffentlichung zu dem Journalisten Kontakt gehabt hat. Entsprechende Daten werden aber nicht gefunden. Das Verfahren gegen A wird eingestellt. Sie will nunmehr die Rechtswidrigkeit der Maßnahme feststellen lassen. Das Landgericht lehnt ihren Antrag ab. Daraufhin erhebt sie Verfassungsbeschwerde.

[1] Der im Folgenden wiedergegebene Sachverhalt beschränkt sich auf die Angaben, die zur Erörterungen der Fallprobleme notwendig sind.

2. Problem(e) und bisheriger Meinungsstand

Auf dem Weg zum Hauptproblem muss eine Hürde prozessualer Art genommen werden. Es könnte am **Rechtsschutzbedürfnis** fehlen, weil sich die Sache erledigt hat. Und zwar genau genommen schon dadurch, dass die beanstandete Durchsuchungs- und Beschlagnahmeanordnung ausgeführt wurde, also nicht mehr aufgehoben werden kann, falls sie sich als rechtswidrig erweist. Nun ist aber genau das – nämlich die sofortige Ausführung, welche die Wahrnehmung eines Rechtsbehelfs ausschließt, – typisch für strafprozessuale Zwangsmaßnahmen.

Ein Rechtsstaat muss auch in diesen Fällen Rechtsschutz gewähren. Also nachträglich.[2] Das ist jedenfalls für tief greifende Grundrechtseingriffe anerkannt, insbesondere für solche, die grundgesetzlich unter Richtervorbehalt stehen.[3] Das prozessual richtige Mittel ist der – hier auch gestellte – Feststellungsantrag, der darauf zielt, die Rechtswidrigkeit der Maßnahme bestätigt zu erhalten.

Im vorliegenden Fall sind die Voraussetzungen erfüllt, weil auf jeden Fall das Grundrecht der Unverletzlichkeit der Wohnung betroffen ist, dessen Beeinträchtigung im Wege der Durchsuchung in der Regel eine richterliche Anordnung erfordert (Art. 13 Abs. 2 GG).

Für die weitere Fallbearbeitung, die sich mit der Frage einer etwaigen Rechtswidrigkeit der Durchsuchungs- und Beschlagnahmeanordnung befasst, tritt Art. 13 GG zunächst in den Hintergrund. Denn es gibt eine Möglichkeit, mit Hilfe eines anderen Grundrechts zu einer raschen Lösung zu gelangen, indem die Rechtswidrigkeit mit einer allgemeinen Erwägung begründet wird, die nicht von den jeweiligen Fallumständen abhängt. Gemeint ist das **Fernmeldegeheimnis nach Art. 10 Abs. 1 GG**. Dieses Grundrecht kann hier tangiert sein, weil die landgerichtliche Anordnung die Erlangung von Kommunikationsdaten bezweckte.

Strafprozessrechtliche Eingriffe in Art. 10 Abs. 1 GG sind gesetzlich eng begrenzt, was den **hohen verfassungsrechtlichen Rang** des Grundrechts deutlich macht. Im Hinblick auf die hier relevante Telekommunikation regelt die StPO deren Überwachung und Aufzeichnung (§§ 100 a und b StPO) sowie die Erlangung von Auskünften der Telekommunikationsdiensteanbieter (§§ 100 g und h StPO). Jeweils ist die Anordnung nur zulässig, wenn sich der Verdacht auf eine der gesetzlich ausdrücklich genannten, erheblichen Straftaten bezieht.[4] Auch ist der Kreis der Anordnungsbefugten auf Richter und (bei Gefahr im Verzug) Staatsanwälte beschränkt. Eine Anordnung durch Polizeibeamte ist damit ausgeschlossen.

Diese Regelungen erfassen den hier vorliegenden Fall einer Erlangung von Telekommunikationsdaten beim Teilnehmer allerdings nicht unmittelbar. Denn der Kommunikationsvorgang war bereits abgeschlossen; auch wurden keine Daten von einem Diensteanbieter abgefragt. Die in den genannten Vorschriften vorgesehenen Grenzen könnten aber auf unseren Fall zu übertragen sein. Argument: In vergleichbarer Weise ist die Telekommunikation betroffen; also müssen gleichermaßen die aus dem Fernmeldegeheimnis abgeleiteten Grenzen gelten. Folge: Rechtswidrig sind alle Maßnahmen dieser Art sowie darauf zielende Durchsuchungs- und Beschlagnahmebeschlüsse, die sich nicht auf den Verdacht einer Katalogtat beziehen. Nicht zu den Katalogtaten gehört die hier in Betracht kommende Verletzung eines Dienstgeheimnisses nach § 353 b Abs. 1 StGB.

Soll diese Gleichsetzung überzeugen, so bedarf sie näherer Begründung. Diese könnte so aussehen:[5]

Art. 10 Abs. 1 GG schützt die Vertraulichkeit der Telekommunikation. Sie ist auch beeinträchtigt, wenn auf gespeicherte Verbindungsdaten zugegriffen werden kann, welche Rückschlüsse auf die Art, die Häufigkeit, die Dauer, die Zeitpunkte und die Beteiligten zulassen. Dementsprechend wird ja auch gesetzlich durch §§ 100 g und h StPO

---

[2] Das Erfordernis eines auch nachträglich zu gewährenden Rechtsschutzes gegen prozessualen Zwang wird aus § 28 Abs. 1 Satz 4 EGGVG abgeleitet; vgl. *Beulke*, Strafprozessrecht, 8. Aufl. 2005, Rn. 327.

[3] Vgl. BVerfGE 96, 27, 38 ff.; 104, 220, 233; *Beulke* (Fn. 2), Rn. 327.

[4] Der Katalog dieser Straftaten findet sich in § 100 a Satz 1 StPO. Auf ihn verweist § 100 g Abs. 1 Satz 1 StPO.

[5] Die hier angeführten Argumente finden sich u. a. in dem am Ende von 2. erwähnten Kammerbeschluss des BVerfG NStZ 2005, 237, sowie in der Stellungnahme des Anwaltsvereins zum vorliegenden Verfahren, veröffentlicht unter www.anwaltsverein.de (Stellungnahme Nr. 45/2005).

der Zugriff auf solche Daten eingeschränkt, die sich im Herrschaftsbereich von Telekommunikationsdiensteanbietern befinden. Es sollte den Strafverfolgungsorganen nicht ermöglicht werden, diese Schranken zu umgehen, indem sie ohne Rücksicht darauf entsprechende Daten im Herrschaftsbereich der Teilnehmer sicherstellen dürfen. Im Übrigen spricht § 88 Abs. 1 TKG für eine Erstreckung des Fernmeldegeheimnisses auf Verbindungsdaten im Teilnehmerbereich. Danach unterliegen dem Fernmeldegeheimnis auch die näheren Umstände der Telekommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Die Vorschrift enthält keine Einschränkung auf Daten, die sich im Herrschaftsbereich von Telekommunikationsdiensten befinden.

Diesen Argumenten steht als Haupteinwand gegenüber, dass nach gängiger Lesart Art. 10 Abs. 1 GG die Kommunikation selbst schützt, woraus abgeleitet wird, dass mit dem Übertragungsvorgang auch der grundrechtliche Schutz endet.[6] Damit stimmt zwar nicht überein, dass §§ 100 g und h StPO mit ihren erhöhten Anforderungen eine Erweiterung dieses Schutzes auf gespeicherte Verbindungsdaten bei den Telekommunikationsdiensten vorsehen. Doch lässt sich diese Ausdehnung des Schutzes damit erklären, dass Zugriffe auf diese „geronnene" Kommunikation gleichermaßen wie diejenigen auf die unmittelbare Kommunikation dem Teilnehmer verborgen bleiben, was nicht für Zugriffe auf Verbindungsdaten in seinem Herrschaftsbereich gilt.[7]

Wird der zuletzt dargestellte Standpunkt eingenommen, so begründet nicht schon das Fehlen einer Katalogtat die Rechtswidrigkeit der Maßnahme. Außerdem scheidet Art. 10 Abs. 1 GG für die weitere verfassungsrechtliche Prüfung aus. Zu untersuchen sind Grundrechtsverletzungen sonstiger Art. Dabei ist an die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) und an das verfassungsgerichtlich entwickelte Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG)[8] zu denken. Eine gleichermaßen generelle Lösung wie beim Grundrecht des Fernmeldegeheimnisses kommt nicht in Betracht. Jeweils wird es – insbesondere im Hinblick auf die Frage der Verhältnismäßigkeit – auf die Umstände des Einzelfalles ankommen.

Zu erwarten war im vorliegenden Fall aber eher eine gegenläufige Entscheidung. Denn in einem Kammerbeschluss in anderer Sache hatte das Bundesverfassungsgericht den Anwendungsbereich des Fernmeldegeheimnisses auch auf die Sicherstellung von Verbindungsdaten beim Beschuldigten erstreckt und dementsprechend die Rechtmäßigkeit strafprozessualer Zwangsmaßnahmen von der Einhaltung der Anforderungen der §§ 100 g und h StPO abhängig gemacht.[9]

3. Kernaussagen der Entscheidung

Überraschend entscheidet sich der Senat in der Grundsatzfrage – Reichweite des Fernmeldegeheimnisses – jedoch anders als die Kammer.[10] §§ 93 a bis c BVerfGG ist zu entnehmen, dass Grundsatzfragen im Zusammenhang mit Verfassungsbeschwerden von den Senaten zu entscheiden sind. Daher ist die Senatsentscheidung als verbindlich zu betrachten.

Die Verfassungsbeschwerde der A hat gleichwohl Erfolg. Der Senat gibt ihr

---

6 Vgl. z. B. *Gusy* in v. Mangoldt/Klein/Starck, Grundgesetz, 5. Aufl. 2005, Art. 10 Rn. 24; *Bär*, MMR 2005, 523 f.

7 So z. B. *Hauschild* NStZ 2005, 539 f.; *Bär,* MMR 2005, 523 f.

8 BverfGE 65, 1 ff. (Volkszählungsurteil); vgl. dazu *Ipsen*, Staatsrecht II, Grundrechte, 8. Aufl. 2005, Rn. 294 ff.

9 BVerfG NStZ 2005, 337.

10 Wer mit dem Aufbau des Bundesverfassungsgerichts nach Senaten und Kammern nicht vertraut ist, kann sich Grundinformationen über die Internetseite des Gerichts (www.bundesverfassungsgericht.de) verschaffen.

mit der Begründung statt, dass die landgerichtliche Durchsuchungs- und Beschlagnahmeanordnung unverhältnismäßig gewesen sei.

Die Entscheidungsbegründung folgt einer Drei-Schritte-Struktur: Ja – aber – aber.

Ja: Der Schutzbereich von Art. 10 Abs. 1 GG erstreckt sich über den Kommunikationsvorgang hinaus auch auf datenmäßig fixierte Umstände der Kommunikation. Aber: Der Schutz besteht nicht für Daten, die vom Teilnehmer beherrschbar sind. Aber: Solche im Herrschaftsbereich des Teilnehmers befindliche Daten werden grundrechtlich nicht allein durch das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG), sondern zusätzlich durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) geschützt, dem hier erhebliches Gewicht zukommt, weil es insoweit eine „Ergänzungsfunktion zu Art. 10 GG“[11] hat.

Auf dieser Grundlage wird den gesetzlichen Regelungen der StPO über die Durchsuchung und die Beschlagnahme attestiert, dass sie auch im Hinblick auf die Sicherstellung von Telekommunikationsdaten beim Teilnehmer verfassungsrechtlich unbedenklich seien, weil sich insoweit keine erhöhten Anforderungen aus Art. 10 Abs. 1 GG ergäben.

Bei der Überprüfung der konkreten Maßnahme am Maßstab des Grundrechts auf informationelle Selbstbestimmung sowie des Grundrechts auf Unverletzlichkeit der Wohnung wird ein Verstoß gegen die Anforderungen des Verhältnismäßigkeitsprinzips festgestellt: Dem geringgewichtigen Verdacht einer nicht sonderlich schweren Straftat habe ein schwerwiegender Eingriff gegenübergestanden, der zudem angesichts des verstrichenen Zeitraums von fünf Monaten nur wenig aussichtsreich gewesen sei.

Für die Entscheidung des Grundsatzproblems ist die **unterschiedliche Behandlung der Verbindungsdaten je nach dem Ort der Speicherung** von zentraler Bedeutung. Das Bundesverfassungsgericht sieht sich hier genötigt, das Argument, mit dem es Daten im Herrschaftsbereich des Teilnehmers dem Schutz durch Art. 10 Abs. 1 GG entzieht, gegen Einwände abzusichern. Es ist nämlich sehr zweifelhaft, ob es tatsächlich in der Hand des Teilnehmers liegt, die bei ihm befindlichen Daten vor dem Zugriff Dritter, z. B. durch Löschung, zu sichern. Die Sachverständigenanhörung vor dem Bundesverfassungsgericht hat ergeben, dass ein zuverlässiger Schutz für den durchschnittlichen Teilnehmer technisch kaum zu bewerkstelligen ist. Die bloße Betätigung der Löschtaste genügt jedenfalls nicht.

Diesem Einwand begegnet das Gericht – wenig überzeugend – mit einem Brachial-Argument: Jedenfalls die „physische Zerstörung des Datenträgers“[12] sei möglich. Ferner führt es einen Vergleich an, der das Problem der Beherrschbarkeit aber ungelöst lässt. Maßgeblich sei eine Vergleichbarkeit mit den sonst in der Privatsphäre des Nutzers gespeicherten Daten, etwa dem selbst angelegten Rufnummernverzeichnis in einem Telefongerät oder den auf einer Computerfestplatte abgelegten Informationen. Wie für diese so seien auch für die gespeicherten Verbindungsdaten die „spezifischen Risiken eines der Kontroll- und Einwirkungsmöglichkeit des Teilnehmers entzogenen Übertragungsvorgangs“[13] nicht mehr gegeben.

Erwähnenswert ist schließlich noch die **kriminalpolitische Argumentation** in der Entscheidung, die den Ausschlag dafür gegeben haben dürfte, dass der Senat anders als die Kammer entschieden hat. Der Senat hat sich überzeugen lassen von „in der Ermittlungspraxis erfahrenen Auskunftspersonen“[14], die davor gewarnt haben, die

[11] BVerfG NJW 2006, 976, 979.

[12] BVerG NJW 2006, 976, 979.

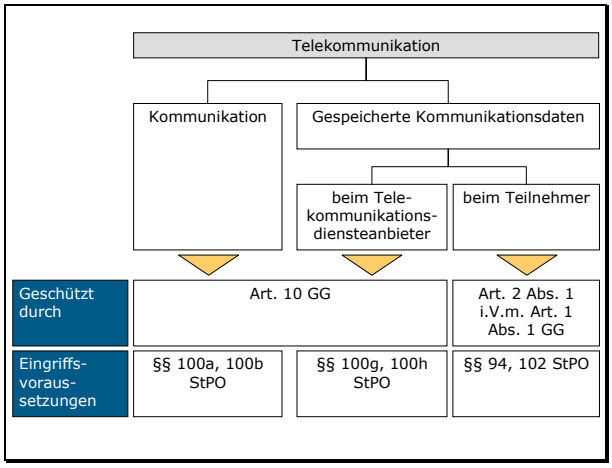
[13] BVerG NJW 2006, 976, 979.

[14] BVerG NJW 2006, 976, 981.

Sicherstellung von Verbindungsdaten bei Teilnehmern auf Fälle des Verdachts erheblicher Straftaten zu begrenzen. Ein Zugriff müsse auch unabhängig vom Straftatenkatalog in § 100 a Abs. 1 Satz 1 StPO möglich sein, etwa in Fällen der Pornografie oder der Wirtschaftskriminalität. Nur so sei ein „Schritthalten der Strafverfolgungsbehörden mit dem technischen Fortschritt“[15] zu gewährleisten.

4. Konsequenzen für Ausbildung und Praxis

Der Fall verbindet Verfassungsrecht und Strafprozessrecht. Dementsprechend sollte auch eine systematische Erfassung des Hauptproblems die beiden Rechtsgebiete zusammenführen. Wir versuchen es mit der folgenden Übersicht, welche bereits das Ergebnis der vorliegenden Entscheidung verarbeitet.



Die Rechtsprobleme des Falles können im Prüfungszusammenhang als verfassungsrechtliche oder als strafprozessrechtliche Aufgabenstellung auftreten. Wir wollen uns hier etwas näher mit den Anforderungen an eine strafprozessrechtliche Bearbeitung befassen.

Zu erwarten ist, dass die Aufgabe eine Beurteilung der Rechtslage schon in einem früheren Verfahrensstadium verlangt, etwa durch die Aufforderung, die Rechtmäßigkeit der Durchsuchungs- und Beschlagnahmeanordnung oder die Möglichkeiten und Erfolgsaussichten eines Rechtsbehelfs gegen die Anordnung (vor oder nach der Ausführung der Maßnahme) zu prüfen.

Das ändert allerdings nichts an der Relevanz des Verfassungsrechts, das schon bei der Prüfung der Zulässigkeit eines Rechtsbehelfs, etwa bei der Untersuchung des Rechtsschutzinteresses,[16] auf jeden Fall aber bei der Prüfung der Begründetheit zu berücksichtigen ist.

Für eine erfolgreiche Bearbeitung sind Grundkenntnisse über das **System der Rechtsbehelfe** gegenüber strafprozessrechtlichen Zwangseingriffen im Ermittlungsverfahren nötig.[17] Liegt eine noch nicht erledigte richterliche Anordnung vor und will sich der Betroffene gegen ihren Erlass wehren,[18] so sollte er Beschwerde gem. § 304 StPO einlegen. Bei Anordnungen durch die Staatsanwaltschaft oder deren Ermittlungspersonen kann gem. § 98 Abs. 2 Satz 2 StPO eine gerichtliche Entscheidung herbeigeführt werden, die dann wiederum mit der Beschwerde angefochten werden kann. Gleiches gilt nach Erledigung der Maßnahme; allerdings bedarf es im Hinblick auf § 98 Abs. 2 Satz 2 StPO der Analogie.

Häufig wird auch die Frage auftreten, welche Folgen die festgestellte Rechtswidrigkeit des Eingriffs für die Verwertung der erlangten Beweise hat. Ob ein **Beweisverwertungsverbot** eingreift, muss gesondert geprüft werden.[19] Soweit die Verwertung nicht ausdrücklich gesetzlich verboten ist, hängt die Verwertbarkeit nach h. M. von einer Einzelfallprüfung ab, in der abzuwägen ist zwischen dem Interesse

[15] BVerG NJW 2006, 976, 981.

[16] Siehe oben 2.

[17] Vgl. zum Folgenden die Darstellung mit Übersicht bei *Beulke* (Fn. 2), Rn. 321 ff.

[18] Daneben sind Rechtsbehelfe möglich, die sich gegen die Art und Weise der Durchführung wenden; vgl. auch dazu *Beulke* (Fn. 2), Rn. 321 ff.

[19] Vgl. dazu und zum Folgenden *Volk*, Grundkurs StPO, 4. Aufl. 2005, § 28, sowie die folgenden FAMOS-Fälle: Brechmittel-Fall (April 2002), Folter-Fall (September 2003) und Selbstgesprächs-Fall (Oktober 2005).

an der Wahrheitsfindung und an einer effektiven Strafverfolgung einerseits und der (auch verfassungsrechtlichen!) Bedeutung des verletzten Interesses. Ein Verwertungsverbot wird in der Regel bei schwerwiegenden, bewussten oder willkürlichen Verstößen gegen Verfahrensvorschriften angenommen, die dem Schutz der verfahrensrechtlichen Stellung des Beschuldigten dienen.

Für die Praxis bedeutet die Entscheidung, dass schwer vorherzusagen ist, wie die Sicherstellung von Verbindungsdaten bei Telekommunikationsteilnehmern von den Gerichten beurteilt wird. Da die Einschränkungen der §§ 100 g und h StPO nicht zum Zuge kommen, hängt alles von der Beurteilung der Verhältnismäßigkeit im Einzelfall ab.

5. Kritik

Die unmittelbar am Verfahren Beteiligten und von ihm Betroffenen werden mit dessen Ausgang zufrieden gewesen sein. Die Beschwerdeführerin hat im Ergebnis Recht bekommen. Die staatlichen Strafverfolgungsorgane sind von den Fesseln befreit worden, die ihnen die vorangegangen Kammerentscheidung angelegt hatte.

Ob auch von einem allgemeinen Rechtsstandpunkt aus Zufriedenheit angebracht ist, erscheint uns zweifelhaft. Auf den Gesichtspunkt mangelnder Vorhersehbarkeit künftiger Gerichtsentscheidungen haben wir bereits hingewiesen. Hinzu kommt, dass das Kernargument – Beherrschbarkeit der Daten für den Teilnehmer – realitätsfremd ist, weil der durchschnittliche Teilnehmer nicht den technischen Sachverstand besitzt, um die Herrschaft über die gespeicherten Daten tatsächlich uneingeschränkt ausüben zu können.

Ein Schlusswort zur Hypertrophie bundesverfassungsgerichtlicher Entscheidungsbegründungen. Wie die Bürger dieses Landes, so werden auch die Entscheidungen seines höchsten Gerichts immer dicker. Die vorliegende Entscheidung mit einem Umfang von mehr als 80.000 Zeichen treibt eine Entwicklung weiter voran, die auf die Dimension einer Monografie mittleren Umfangs zusteuert. Da die Fähigkeit, sich kurz und prägnant auszudrücken, offenbar nicht zu den Kriterien der Personalauswahl gehört und das Bundesverfassungsgericht über kein Lektorat verfügt, muss der Verbraucher sich selbst schützen. Zwei Ratschläge dazu von unserer Seite. Es empfiehlt sich, zunächst, wenn vorhanden, die Pressemitteilung des Gerichts über die Entscheidung zu lesen. Sie gibt zumeist in prägnanter Kürze den wesentlichen Inhalt wieder. Auch kann man bei der Lektüre der Entscheidung häufig die berichtenden Passagen, die vielfach die Hälfte des Gesamtumfangs ausmachen, überspringen, ohne dass sich Verständnisprobleme ergeben.

(Dem Text liegen Entwürfe von Christopher Jones und Julia Schubert zugrunde. Die Grafik hat Nicola Pridik angefertigt.)