I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (*Anti-Counterfeiting Trade Agreement*, ACTA)

(2010/C 147/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1],

gestützt auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [2],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [3], insbesondere auf Artikel 41—

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Die Europäische Union nimmt an den Verhandlungen zur Ausarbeitung eines Abkommens zur Bekämpfung von Produkt- und Markenpiraterie (*Anti-Counterfeiting Trade Agreement*, ACTA) teil. Diese Verhandlungen wurden im Jahr 2007 von einer anfänglichen Gruppe interessierter Parteien aufgenommen und dann mit einer größeren Gruppe von Teilnehmern fortgeführt; bis jetzt gehören dazu Australien, Kanada, die Europäische Union, Japan, Korea, Mexiko, Marokko, Neuseeland, Singapur, die Schweiz und die Vereinigten Staaten. Die Europäische Kommission erhielt im Jahr 2008 vom Rat das Mandat, diesen Verhandlungen beizutreten.

2. Der EDSB räumt ein, dass der grenzüberschreitende Handel mit nachgeahmten und gefälschten Waren, an dem oftmals Netzwerke der organisierten Kriminalität beteiligt sind, immer mehr Anlass zur Besorgnis gibt und die Annahme geeigneter Mechanismen für die Zusammenarbeit auf internationaler Ebene erfordert, um gegen diese Form der Kriminalität vorzugehen.

3. Der EDSB legt dar, dass die Aushandlung eines multilateralen Abkommens durch die Europäische Union, dessen Kernpunkt die stärkere Durchsetzung von Rechten des geistigen Eigentums ist, signifikante Fragen hinsichtlich der Auswirkungen der zur Bekämpfung der Produktfälschung und -piraterie ergriffenen Maßnahmen auf die Grundrechte natürlicher Personen aufwirft — insbesondere auf deren Recht auf Schutz der Privatsphäre und auf Datenschutz.

4. In diesem Zusammenhang bedauert der EDSB insbesondere, dass er von der Europäischen Kommission nicht hinsichtlich des Inhalts eines solchen Abkommens konsultiert wurde. Gestützt auf Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 hat der EDSB daher auf eigene Initiative die vorliegende Stellungnahme angenommen, um der Kommission Orientierungshilfen in Bezug auf die in den ACTA-Verhandlungen zu berücksichtigenden Aspekte in den Bereichen Privatsphäre und Datenschutz an die Hand zu geben.

II. STAND DER VERHANDLUNGEN UND VORAUSSICHTLICHER INHALT DES ACTA

5. Die 7. Verhandlungsrunde fand vom 26. bis 29. Januar 2010 in Mexiko statt. Angestrebt wird der Abschluss eines Abkommens im Verlauf des Jahres 2010; bis jetzt wurde jedoch noch kein offizieller Entwurf des Abkommens freigegeben.

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 201 vom 31.7.2002, S. 37.
[3] ABl. L 8 vom 12.1.2001, S. 1.

6. Das Ziel der Verhandlungen ist die Annahme eines neuen plurilateralen Abkommens zur stärkeren Durchsetzung von Rechten des geistigen Eigentums und zur Bekämpfung der Produktfälschung und -priraterie. Im Falle seiner Annahme würde dieses neue Abkommen zu verbesserten internationalen Standards für das Vorgehen gegen groß angelegte Verletzungen von Rechten des geistigen Eigentums führen. Die GD Handel der Europäischen Kommission hat insbesondere erläutert, dass der beabsichtigte Schwerpunkt eher auf Tätigkeiten im Bereich Produktfälschung und -piraterie, die gewerbliche Interessen erheblich beeinträchtigen, als auf den Tätigkeiten normaler Bürger liegt („the intended focus is on counterfeiting and piracy activities that significantly affect commercial interests, rather than on activities of ordinary citizens") ([4]).

7. Was den Inhalt des Abkommens anbelangt, ist der von der GD Handel der Europäischen Kommission im November 2009 herausgegebenen Zusammenfassung der zur Diskussion stehenden Kernaspekte (*Summary of key elements under discussion*) zu entnehmen, dass das Ziel des ACTA, nämlich die Bekämpfung von Produktpiraterie und -fälschung, durch drei primäre Komponenten verfolgt werden wird: i) internationale Zusammenarbeit, ii) Durchsetzungsverfahren und iii) Festlegung eines Rechtsrahmens für die Durchsetzung von Rechten des geistigen Eigentums in mehreren ermittelten Bereichen, insbesondere im digitalen Umfeld ([5]). Die vorgesehenen Maßnahmen werden sich insbesondere mit rechtlichen Verfahren (wie gerichtliche Anordnungen, einstweilige Maßnahmen), mit der Rolle und den Zuständigkeiten von Internet-Diensteanbietern in Bezug auf die Abschreckung von Verletzungen des Urheberrechts über das Internet sowie mit grenzüberschreitenden Kooperationsmaßnahmen zur Verhinderung des Grenzübertritts von Waren befassen. Die veröffentlichten Informationen umreißen den Inhalt des Abkommens jedoch nur in großen Zügen und enthalten keine Angaben zu Details spezifischer und konkreter Maßnahmen.

8. Der EDSB merkt an, dass — auch wenn nur die Verfolgung groß angelegter Verletzungen von Rechten des geistigen Eigentums beabsichtigtes Ziel des ACTA ist — nicht ausgeschlossen werden kann, dass im Rahmen des ACTA auch Tätigkeiten normaler Bürger erfasst werden, insbesondere wenn Durchsetzungsmaßnahmen im digitalen Umfeld erfolgen. Der EDSB betont, dass dies die Festlegung geeigneter Garantien zum Schutz der Grundrechte natürlicher Personen erfordern wird. Überdies gelten Datenschutzgesetze für alle natürlichen Personen — auch für Personen, die potenziell an Tätigkeiten im Bereich Produktfälschung und -piraterie beteiligt sind; die Bekämpfung groß angelegter Verletzungen von Rechten wird mit Sicherheit auch die Verarbeitung personenbezogener Daten einschließen.

9. Diesbezüglich bestärkt der EDSB die Europäische Kommission entschieden darin, einen öffentlichen und transparenten Dialog über das ACTA aufzunehmen, möglicherweise im Wege einer öffentlichen Konsultation; dies würde auch dazu beitragen, dass sichergestellt wird, dass die zu erlassenden Maßnahmen den Anforderungen des EU-Rechts im Bereich der Privatsphäre und des Datenschutzes entsprechen.

III. UMFANG DER KOMMENTARE DES EDSB

10. Der EDSB appelliert eindringlich an die EU, insbesondere an die Europäische Kommission, die das Mandat zum Abschluss des Abkommens erhalten hat, den richtigen Mittelweg zwischen den Forderungen nach Schutz von Rechten des geistigen Eigentums und dem Recht natürlicher Personen auf Schutz der Privatsphäre und auf Datenschutz zu finden.

11. Der EDSB betont, dass das Recht auf Privatsphäre und der Datenschutz zentrale Werte der Europäischen Union darstellen, die in Artikel 8 EMRK und in den Artikeln 7 und 8 der Charta der Grundrechte der EU ([6]) verankert und gemäß Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) in allen Politikbereichen und bei allen Vorschriften der EU zu wahren sind.

12. Ferner betont der EDSB, dass jegliche Vereinbarungen der Europäischen Union zum ACTA den rechtlichen Verpflichtungen der EU im Hinblick auf den Schutz der Privatsphäre und den Datenschutz entsprechen müssen, wie sie insbesondere in den Richtlinien 95/46/EG ([7]) und 2002/58/EG ([8]) sowie in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ([9]) und des Gerichtshofs der Europäischen Union niedergelegt sind.

13. Privatsphäre und Datenschutz müssen von Beginn der Verhandlungen an berücksichtigt werden, nicht erst wenn die Regelungen und Verfahren festgelegt und vereinbart wurden und es somit zu spät für alternative, dem Recht auf Privatsphäre gerecht werdende Lösungen ist.

14. In Anbetracht der wenigen Informationen, die der Öffentlichkeit zugänglich gemacht werden, merkt der EDSB an, dass er nicht in der Lage ist, eine Analyse der spezifischen Bestimmungen des ACTA vorzunehmen. In dieser Stellungnahme konzentriert sich der EDSB daher auf die Darstellung der potenziellen Gefahren etwaiger konkreter Maßnahmen für die Privatsphäre und den Datenschutz, zu denen das Abkommen Berichten zufolge in den beiden folgenden Bereichen möglicherweise führen wird: Durchsetzung von Rechten des geistigen Eigentums im digitalen Umfeld (Kapitel IV) und Mechanismen der internationalen Zusammenarbeit (Kapitel V).

([4]) Siehe http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, S. 2.

([5]) Siehe Fußnote 2.

([6]) Charta der Grundrechte der Europäischen Union, ABl. C 303 vom 14.12.2007, S. 1.

([7]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

([8]) Auslegung der wichtigsten Elemente und Bedingung von Artikel 8 der am 4. November 1950 in Rom angenommenen Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) und ihrer Geltung für verschiedene Bereiche. Siehe insbesondere die Rechtsprechung, auf die an anderer Stelle in dieser Stellungnahme verwiesen wird.

([9]) Siehe insbesondere: Rechtssache C-275/06, *Productores de Música de España* (Promusicae), Slg. 2008, I-271, und Rechtssache C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, noch nicht in die Sammlung aufgenommen.

IV. DURCHSETZUNG VON RECHTEN DES GEISTIGEN EIGENTUMS IM DIGITALEN UMFELD

IV.1 Notwendigkeit einer Analyse der Auswirkungen von Three-Strikes-Internetsperren auf die Privatsphäre bzw. den Datenschutz

15. Der Europäischen Kommission zufolge wird das ACTA einen Rechtsrahmen für die Bekämpfung von Piraterie im digitalen Umfeld schaffen ([10]) Dieser Rahmen wird die Bedingungen festlegen, unter denen Internet-Diensteanbieter und andere Online-Vermittler ([11]) für gegen das Urheberrecht verstoßendes Material, das über ihre Einrichtungen übermittelt wird, verantwortlich gemacht werden können. Der Rahmen kann auch Maßnahmen und Abhilfemaßnahmen vorsehen, die gegen Internet-Nutzer verhängt werden können, die gegen das Urheberrecht verstoßendes Material hoch- oder heruntergeladen haben. Zwar wurden die Details eines solchen Rahmens noch nicht offiziell freigegeben, in Anbetracht der über verschiedene Kanäle bekannt gewordenen Informationen ist jedoch davon auszugehen, dass er für Internet-Diensteanbieter die Verpflichtung beinhalten wird, Three-Strikes-Internetsperren (auch als System der abgestuften Erwiderung oder „graduated response"-Regelungen bezeichnet) einzuführen. Solche Regelungen werden Urheberrechtsinhabern die Möglichkeit bieten, Internet-Nutzer zu überwachen und mutmaßliche Urheberrechtsverletzer zu identifizieren. Nachdem ein Kontakt zu den Internet-Diensteanbietern des mutmaßlichen Rechtsverletzers hergestellt wurde, würden diese den als Rechtsverletzer identifizierten Nutzer verwarnen; nach drei Verwarnungen würde sein Internetzugang gesperrt werden.

16. Parallel zu den ACTA-Verhandlungen werden in manchen Mitgliedstaaten, beispielsweise Frankreich, *Three-Strikes*-Internetsperren umgesetzt. Diese werden auch in diversen Foren der EU erörtert, beispielsweise im Rahmen des *Stakeholders' Dialogue on illegal up- and downloading* (Dialog der beteiligten Akteure über illegales Up- und Downloading), der derzeit auf Initiative der GD MARKT stattfindet, in Verbindung mit der Annahme der Mitteilung der Kommission über die Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt ([12]) Erörterungen zu diesem Thema finden auch im Europäischen Parlament statt, und zwar im Kontext der anstehenden Debatte über den Entwurf einer Entschließung des Europäischen Parlaments über die Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt (bezeichnet als „Gallo-Bericht").

17. Solche Praktiken stellen schwere Eingriffe in die Privatsphäre natürlicher Personen dar. Sie ziehen die generalisierte Überwachung der Tätigkeiten von Internetnutzern nach sich — selbst völlig rechtmäßiger Tätigkeiten. Sie wirken sich auf Millionen gesetzestreuer Internetnutzer aus, darunter auch viele Kinder und Jugendliche. Sie werden von privaten Parteien durchgeführt, nicht von Strafverfolgungsbehörden. Zudem spielt das Internet heutzutage eine zentrale Rolle in fast allen Aspekten des modernen Lebens; daher können die Auswirkungen einer Sperrung des Internet-Zugangs enorm sein und die Betroffenen am Zugriff auf Anwendungen in den Bereichen Arbeit, Kultur, E-Government usw. hindern.

18. Vor diesem Hintergrund muss beurteilt werden, inwieweit diese Verfahren mit den Rechtsvorschriften der EU in den Bereichen Datenschutz und Privatsphäre im Einklang stehen, insbesondere im Hinblick auf die Frage, ob Three-Strikes-Internetsperren eine notwendige Maßnahme zur Durchsetzung von Rechten des geistigen Eigentums darstellen. In diesem Kontext sollte zudem analysiert werden, ob es andere Methoden gibt, die weniger starke Eingriffe nach sich ziehen.

19. Es ist noch immer unklar, ob Three-Strikes-Internetsperren Bestandteil das ACTA sein werden. Diese Verfahren werden jedoch auch in anderen Bereichen in Betracht gezogen und haben — potenziell — enorme Auswirkungen auf den Schutz personenbezogener Daten und der Privatsphäre. Aus diesen Gründen hält der EDSB ihre Erörterung in dieser Stellungnahme für notwendig. Bevor die genannte Analyse vorgenommen wird, wird der EDSB kurz den geltenden Rechtsrahmen in den Bereichen Datenschutz und Privatsphäre beschreiben.

20. Es ist anzumerken, dass Three-Strikes-Internetsperren nicht nur Bedenken in Bezug auf Datenschutz und Privatsphäre aufkommen lassen, sondern auch Fragen in Bezug auf andere Werte, beispielsweise Rechtsstaatsprinzipien und Redefreiheit, aufwerfen. Diese Stellungnahme wird sich jedoch nur mit den Fragen befassen, die mit dem Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen in Zusammenhang stehen.

IV.2 Three-Strikes-Internetsperren und die Anwendung des EU-Rechtsrahmens im Bereich Datenschutz/Privatsphäre

Wie Three-Strikes-Internetsperren ausgelegt sein können

21. Im Wesentlichen würden bei Anwendung von Three-Strikes-Internetsperren Urheberrechtsinhaber, die automatisierte technische Mittel verwenden, die möglicherweise von Dritten bereitgestellt werden, mutmaßliche Urheberrechtsverletzungen ermitteln, indem sie eine Überwachung der Tätigkeiten von Internetnutzern vornehmen, beispielsweise mithilfe der Überwachung von Foren, Blogs oder indem sie in

([10]) Siehe Fußnote 2.

([11]) Die verschiedenen Online-Vermittler können anhand ihrer Funktionen definiert werden. In der Realität übernehmen Vermittler jedoch üblicherweise mehrere dieser Funktionen. Zu den Online-Vermittlern gehören: a) *Zugangsanbieter*: Nutzer stellen die Verbindung zum Netzwerk her, indem sie sich mit dem Server eines Zugangsanbieters verbinden; b) *Netzbetreiber:* Sie stellen die Router zur Verfügung, d.h. die für die Datenübermittlung erforderlichen technischen Einrichtungen; c) *Hostbetreiber*: Sie vermieten Speicherplatz auf ihrem Server, auf den Nutzer oder Inhaltsanbieter Inhalte hochladen können. Nutzer können von einem Online-Dienst, beispielsweise einem Bulletin oder einem P2P-Netzwerk, Material herunterladen bzw. hochladen.

([12]) Mitteilung der Kommission an den Rat, das Europäische Parlament und den Europäischen Wirtschafts- und Sozialausschuss — Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt, 11. September 2009, KOM(2009) 467 endgültig.

Peer-to-Peer-Netzwerken als Tauschbörsennutzer auftreten, um andere Tauschbörsennutzer zu identifizieren, die mutmaßlich urheberrechtlich geschütztes Material austauschen ([13]).

22. Nach der Identifizierung von mutmaßlich an Urheberrechtsverletzungen beteiligten Internetnutzern durch Erfassung ihrer Internetprotokolladressen (IP-Adressen) würden Urheberrechtsinhaber die IP-Adressen dieser Nutzer an die entsprechenden Internet-Diensteanbieter übermitteln, die ihre jeweiligen Teilnehmer, denen die entsprechenden IP-Adressen gehören, wegen ihrer potenziellen Beteiligung an Urheberrechtsverletzungen verwarnen würden. Eine mehrmalige Verwarnung durch den Internet-Diensteanbieter würde automatisch dazu führen, dass der Internet-Diensteanbieter den Internet-Anschluss des Teilnehmers kündigt oder sperrt ([14]).

Der anwendbare EU-Rechtsrahmen im Bereich Datenschutz/Privatsphäre

23. Three-Strikes-Internetsperren müssen den aus dem Recht auf Privatsphäre resultierenden Anforderungen nach Artikel 8 EMRK und Artikel 7 der Charta der Grundrechte sowie den Anforderungen gemäß dem in Artikel 8 der Charta der Grundrechte und Artikel 16 AEUV festgeschriebenen und durch Richtlinie 95/46/EG und Richtlinie 2002/58/EG näher ausgeführten Recht auf Datenschutz entsprechen.

24. Nach Ansicht des EDSB stellt die Überwachung des Verhaltens von Internetnutzern und die weitere Erfassung ihrer IP-Adressen einen Eingriff in deren Recht auf Achtung ihres Privatlebens und ihres Schriftwechsels dar — mit anderen Worten einen Eingriff in deren Recht auf Privatleben. Diese Ansicht steht im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ([15]).

25. Richtlinie 95/46/EG ist anwendbar ([16]), da die Three-Strikes-Internetsperren die Verarbeitung von IP-Adressen beinhalten, die — zumindest unter den gegebenen Umständen — als personenbezogene Daten zu betrachten sind. IP-Adressen sind Kennungen in Form einer durch Punkte getrennten Zahlenreihe, beispielsweise 122.41.123.45. Durch eine Anmeldung bei einem Internet-Zugangsanbieter erhält der Teilnehmer Zugang zum Internet. Immer, wenn der Teilnehmer ins Internet gehen will, wird ihm über das Gerät, das er für den Zugang zum Internet nutzt (beispielsweise ein Computer), eine IP-Adresse zugewiesen ([17]).

26. Führt ein Nutzer eine bestimmte Tätigkeit aus, beispielsweise das Hochladen von Material ins Internet, kann er von Dritten anhand der verwendeten IP-Adresse identifiziert werden. Ein Beispiel: Der Nutzer mit der IP-Adresse 122.41.123.45 hat am 1. Januar 2010 um 15.00 Uhr mutmaßlich gegen das Urheberrecht verstoßendes Material auf einen P2P-Dienst hochgeladen. Der Internet-Diensteanbieter ist dann in der Lage, eine solche IP-Adresse mit dem Namen des Teilnehmers, dem er diese Adresse zugewiesen hat, zu verknüpfen und so dessen Identität zu ermitteln.

27. Berücksichtigt man die Definition des Begriffs „personenbezogene Daten" in Artikel 2 der Richtlinie 95/46/EG als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer" ([18]), lässt sich nur der Schluss ziehen, dass IP-Adressen und die Informationen über die mit solchen Adressen verknüpften Tätigkeiten in allen hier relevanten Fällen personenbezogene Daten darstellen. Eine IP-Adresse dient nämlich als Kennnummer, mit deren Hilfe der Name des Teilnehmers, dem eine solche IP-Adresse zugewiesen wurde, ermittelt werden kann. Überdies handelt es sich bei den über den Teilnehmer, der Inhaber einer solchen IP-Adresse ist, erhobenen Informationen („er hat am 1. Januar 2010 um 15.00 Uhr bestimmtes Material auf die Website ZS hochgeladen") eindeutig um *Informationen über* die Tätigkeiten einer bestimmbaren natürlichen Person (den Inhaber der IP-Adresse), die infolgedessen ebenfalls als personenbezogene Daten zu betrachten sind.

([13]) Die P2P-Technologie ist eine verteilte Software-Architektur, die einzelnen Rechnern die Verbindung und die direkte Kommunikation mit anderen Rechnern ermöglicht.

([14]) Alternative Sanktionen wären beispielsweise die Einschränkung des Funktionsumfangs des Internet-Anschlusses durch Begrenzung der Verbindungsgeschwindigkeit, des Verbindungsvolumens usw.

([15]) Siehe insbesondere EGMR, 26. Juni 2006, *Weber und Saravia gegen Deutschland* (Beschluss), Nr. 54934/00, Randnr. 77, und EGMR, 1. Juli 2008, *Liberty and others gegen UK*, Nr. 58243/00.

([16]) In Bezug auf die Anwendbarkeit von Richtlinie 95/46/EG folgt der Gerichtshof einem umfassenden Ansatz; seiner Auffassung nach sind deren Bestimmungen im Lichte von Artikel 8 EMRK auszulegen. In seinem Urteil vom 20. Mai 2003, *Rundfunk*, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Randnr. 68, erklärte der Gerichtshof, dass „die Bestimmungen der Richtlinie 95/46/EG, soweit sie die Verarbeitung personenbezogener Daten betreffen, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung des Privatlebens führen kann, im Licht der Grundrechte auszulegen sind, die nach ständiger Rechtsprechung zu den allgemeinen Rechtsgrundsätzen gehören, deren Wahrung der Gerichtshof zu sichern hat".

([17]) Die IP-Adresse, die der Internet-Diensteanbieter einer natürlichen Person zuweist, kann für jedes Surfen im Internet dieselbe sein (bezeichnet als statische IP-Adressen). Andere IP-Adressen sind dynamisch, was bedeutet, dass der Internet-Zugangsanbieter seinen Kunden bei jeder Verbindung mit dem Internet eine andere IP-Adresse zuweist. Offenkundig kann der Internet-Diensteanbieter die IP-Adresse dem Konto des Teilnehmers, dem er die (dynamische oder statische) IP-Adresse zugewiesen hat, zuordnen.

([18]) In Erwägungsgrund 26 wird diese Begriffsbestimmung wie folgt ergänzt: „Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. … ".

28. Die Artikel-29-Datenschutzgruppe teilt diese Ansichten voll und ganz; in einem Arbeitspapier zu Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten erklärte sie, dass es sich bei IP-Adressen, die erhoben wurden, um Rechte des geistigen Eigentums durchzusetzen, d.h. um Internetnutzer zu identifizieren, die mutmaßlich Rechte des geistigen Eigentums verletzt haben, insoweit um personenbezogene Daten handelt, als sie zur Durchsetzung solcher Rechte gegen eine bestimmte natürliche Person verwendet werden ([19]).

29. Auch die Richtlinie 2002/58/EG ist anwendbar, da Three-Strikes-Internetsperren die Erhebung von Verkehrs- und Kommunikationsdaten nach sich ziehen. Richtlinie 2002/58/EG regelt die Verwendung solcher Daten und sieht den Grundsatz der Vertraulichkeit der mit öffentlichen Kommunikationsnetzen erfolgenden Nachrichtenübermittlung sowie der in diesen Nachrichten enthaltenen Daten vor.

IV.3 **Ob Three-Strikes-Internetsperren eine notwendige Maßnahme darstellen**

30. In Artikel 8 EMRK wird der Grundsatz der Notwendigkeit festgelegt, demzufolge eine Maßnahme, die das Recht natürlicher Personen auf Privatsphäre verletzt, nur dann zulässig ist, wenn sie in einer demokratischen Gesellschaft zur Erreichung des legitimen Ziels, das mit ihr verfolgt wird, eine notwendige Maßnahme darstellt ([20]). Der Grundsatz der Notwendigkeit findet sich auch in den Artikeln 7 und 13 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG ([21]). Der Grundsatz erfordert eine Analyse der Verhältnismäßigkeit der Maßnahme, die anhand einer Abwägung der einander gegenüber stehenden Interessen beurteilt werden muss und in den Kontext der demokratischen Gesellschaft als Ganzes gestellt wird ([22]). Er bedingt überdies eine Bewertung der Frage, ob alternative Maßnahmen zur Verfügung stehen, die einen weniger starken Eingriff darstellen.

31. Auch wenn der EDSB einräumt, dass die Durchsetzung von Rechten des geistigen Eigentums wichtig ist, ist er der Ansicht, dass eine Three-Strikes-Internetsperre in ihrer derzeit bekannten Form — die gewisse, allgemein anwendbare Elemente beinhaltet — eine unverhältnismäßige Maßnahme darstellt und daher nicht als notwendige Maßnahme betrachtet werden kann. Der EDSB ist überdies überzeugt, dass es alternative Lösungen gibt, die einen weniger starken Eingriff darstellen, oder dass die geplanten Sperren mit begrenzterem Umfang oder in einer Weise durchgeführt werden können, die einen weniger starken Eingriff darstellt. Auch auf detaillierterer rechtlicher Ebene wirft das Three-Strikes-Konzept Probleme auf. Dieses Fazit wird nachstehend erläutert.

Three-Strikes-Verfahren sind unverhältnismäßig

32. Der EDSB möchte hervorheben, wie weit reichend die verhängten Maßnahmen sind. In diesem Zusammenhang sind die folgenden Aspekte zu erwähnen:

i) die Tatsache, dass die (unbemerkte) Überwachung Millionen natürlicher Personen und *alle* Nutzer betreffen würde, unabhängig davon, ob sie unter Verdacht stehen;

ii) die Überwachung würde die systematische Erfassung von Daten nach sich ziehen, von denen einige zu einer zivil- oder gar strafrechtlichen Verfolgung der Betroffenen führen können; überdies wären einige der erhobenen Informationen als sensible Daten nach Artikel 8 der Richtlinie 95/46/EG einzustufen, die stärkere Garantien erfordern;

iii) die Überwachung wird voraussichtlich zu vielen Fällen falsch positiver Ergebnisse führen. Ob Urheberrechtsverletzungen vorliegen, ist keine einfach mit „Ja“ oder „Nein“ zu beantwortende Frage. Oftmals müssen Gerichte Dutzende von Seiten umfassende Akten mit äußerst erheblichen Mengen an technischen und rechtlichen Details prüfen, um entscheiden zu können, ob eine Urheberrechtsverletzung vorliegt ([23]);

([19]) Artikel-29-Datenschutzgruppe, Arbeitspapier zu Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten (WP 104), angenommen am 18. Januar 2005. Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt. Siehe auch die Stellungnahme 4/2007 der Gruppe zum Begriff „personenbezogene Daten“ (WP 136), angenommen am 20. Juni 2007, insbesondere S. 16.

([20]) Artikel 8 EMRK nimmt ausdrücklich auf die Anforderung Bezug, dass ein Eingriff oder eine Beschränkung „in einer demokratischen Gesellschaft notwendig“ sein muss.

([21]) Nach Artikel 13 der Richtlinie 95/46/EG ist eine Beschränkung nur dann zulässig, wenn sie „notwendig ist für a) die Sicherheit des Staates; b) die Landesverteidigung; c) die öffentliche Sicherheit; d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen; e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten; f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c, d und e genannten Zwecke verbunden sind; g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen“. Artikel 15 der Richtlinie 2002/58/EG verlangt, dass eine solche Beschränkung „gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist“.

([22]) Siehe auch EGMR, 2. August 1984, *Malone gegen Vereinigtes Königreich*, Serie A Nr. 82, S. 32, Randnummer 81 ff., und EGMR, 4. Dezember 2008, *Marper gegen Vereinigtes Königreich* [GC], Nrn. 30562/04 und 30566/04, Randnr. 101 ff.

([23]) Gerichte müssen möglicherweise beurteilen, ob das Material tatsächlich urheberrechtlich geschützt ist, welche Rechte verletzt wurden und ob die Benutzung als lautere Benutzung betrachtet werden kann, und müssen über das anwendbare Recht, den Schadenersatz usw. entscheiden.

iv) die potenziellen *Auswirkungen* der Überwachung, die zu einer Sperrung des Internet-Zugangs führen könnte. Dies würde einen Eingriff in die Meinungsfreiheit, die Informationsfreiheit sowie den Zugang zu Kultur, E-Government-Anwendungen, Marktplätzen, E-Mail und, in manchen Fällen, beruflichen Tätigkeiten natürlicher Personen darstellen. In diesem Zusammenhang muss insbesondere klargestellt werden, dass die Auswirkungen nicht nur der mutmaßliche Rechtsverletzer spüren wird, sondern alle Familienangehörigen, die denselben Internet-Anschluss nutzen, darunter auch Schüler, die das Internet für ihre schulischen Tätigkeiten nutzenl;

v) die Tatsache, dass die Stelle, die die Beurteilung vornimmt und die Entscheidung trifft, typischerweise eine private Stelle sein wird (d.h. die Urheberrechtsinhaber oder der Internet-Diensteanbieter). Der EDSB hat bereits in einer früheren Stellungnahme seine Bedenken hinsichtlich der Überwachung natürlicher Personen durch den privaten Sektor (z.B. Internet-Diensteanbieter oder Urheberrechtsinhaber) in Bereichen, die grundsätzlich der Zuständigkeit von Strafverfolgungsbehörden unterliegen, zum Ausdruck gebracht ([24]).

33. Der EDSB ist nicht davon überzeugt, dass die Vorteile der Maßnahmen die Nachteile in Form der Auswirkungen auf die Grundrechte natürlicher Personen überwiegen. Der Schutz von Urheberrechten ist ein Interesse der Rechteinhaber und der Gesellschaft. Die Einschränkungen der Grundrechte erscheinen jedoch nicht gerechtfertigt, wenn die Schwere des Eingriffs — d.h. die Größenordnung des durch die oben dargelegten Aspekte aufgezeigten Eingriffs in die Privatsphäre — gegen die voraussichtlichen Vorteile abgewogen werden, nämlich das Abschrecken von Verletzungen von Rechten des geistigen Eigentums, bei denen es sich zum großen Teil um geringfügige Rechtsverletzungen handelt. Wie in den Schlussanträgen der Generalanwältin Kokott in der Rechtssache *Promusicae* ausgeführt wird: „Es ist … nicht sicher, dass privates filesharing, insbesondere wenn es ohne Gewinnerzielungsabsicht geschieht, den Schutz von Urheberrechten hinreichend schwer gefährdet, um eine Inanspruchnahme dieser Ausnahme zu rechtfertigen. Inwieweit privates filesharing einen echten Schaden verursacht, ist nämlich umstritten“ ([25]).

34. In diesem Kontext ist auch an die Reaktion des Europäischen Parlaments auf „Three-Strikes-Regelungen“ im Zusammenhang mit der Überarbeitung des Telekommunikationspakets zu erinnern, insbesondere Änderung 138 der Rahmenrichtlinie ([26]). In dieser Änderung wurde festgelegt, dass Beschränkungen der Grundrechte und -freiheiten nur dann auferlegt werden dürfen, wenn sie im Rahmen einer demokratischen Gesellschaft angemessen, verhältnismäßig und notwendig sind, und ihre Anwendung ist angemessenen Verfahrensgarantien im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts zu unterwerfen, einschließlich des Rechts auf effektiven Rechtsschutz und ein faires Verfahren ([27]).

35. Dabei unterstreicht der EDSB zudem, dass alle Einschränkungen der Grundrechte sowohl auf EU-Ebene als auch auf einzelstaatlicher Ebene einer genauen Prüfung unterliegen. In diesem Zusammenhang kann eine Parallele zu der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung ([28]) gezogen werden, die von dem allgemeinen Datenschutzgrundsatz abweicht, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben werden, nicht mehr benötigt werden. Diese Richtlinie verlangt die Vorratsspeicherung von Verkehrsdaten zum Zwecke der Bekämpfung schwerer Straftaten. Es ist anzumerken, dass die Vorratsspeicherung nur für „schwere Straftaten“ zulässig ist, dass die Vorratsspeicherung auf „Verkehrsdaten“ beschränkt ist, was grundsätzlich Informationen über den Inhalt der Kommunikation ausschließt, und dass strenge Garantien angeführt werden. Dennoch sind Zweifel hinsichtlich der Vereinbarkeit dieser Richtlinie mit den Grundrechtestandards aufgekommen; das rumänische Verfassungsgericht entschied, dass eine pauschale Vorratsspeicherung mit den Grundrechten unvereinbar ist ([29]), und vor dem deutschen Bundesverfassungsgericht ist derzeit ein diesbezügliches Verfahren anhängig ([30]).

Existenz anderer Mittel, die weniger starke Eingriffe nach sich ziehen

36. Die obigen Feststellungen werden durch die Tatsache gestärkt, dass es weniger starke Eingriffe nach sich ziehende Mittel gibt, mit denen derselbe Zweck erreicht werden kann. Der EDSB besteht darauf, dass solche weniger starke Eingriffe nach sich ziehenden Modelle geprüft und erprobt werden sollten.

([24]) Stellungnahme des EDSB vom 23. Juni 2008 zum Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien, ABl. C 2 vom 7.1.2009, S. 2.

([25]) Siehe die in Fußnote 8 genannte Rechtssache, Randnr. 106.

([26]) Siehe Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. L 337 vom 18.12.2009, S. 37.

([27]) Der endgültige Wortlaut der so genannten Änderung 138 lautet: „Artikel 1 Absatz 3a: Maßnahmen der Mitgliedstaaten betreffend den Zugang zu oder die Nutzung von Diensten und Anwendungen über elektronische Kommunikationsnetze durch die Endnutzer wahren die in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts verankerten Grundrechte und -freiheiten natürlicher Personen. Alle diese Maßnahmen betreffend den Zugang zu oder die Nutzung von Diensten und Anwendungen über elektronische Kommunikationsnetze durch die Endnutzer, die diese Grundrechte und -freiheiten einschränken können, dürfen nur dann auferlegt werden, wenn sie im Rahmen einer demokratischen Gesellschaft angemessen, verhältnismäßig und notwendig sind, und ihre Anwendung ist angemessenen Verfahrensgarantien im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts zu unterwerfen, einschließlich des Rechts auf effektiven Rechtsschutz und ein faires Verfahren. Dementsprechend dürfen diese Maßnahmen nur unter gebührender Beachtung des Grundsatzes der Unschuldsvermutung und des Rechts auf Schutz der Privatsphäre ergriffen werden. Ein vorheriges, faires und unparteiisches Verfahren, einschließlich des Rechts der betroffenen Person(en) auf Anhörung, wird gewährleistet, unbeschadet des Umstandes, dass in gebührend begründeten Dringlichkeitsfällen geeignete Bedingungen und Verfahrensvorkehrungen im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten notwendig sind. Das Recht auf eine effektive und rechtzeitige gerichtliche Prüfung wird gewährleistet.“

([28]) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006, ABl. L 105 vom 13.4.2006, S. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. In diesem Kontext erinnert der EDSB daran, dass die geänderte Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (als Richtlinie „Rechte der Bürger" bezeichnet), die Bestandteil des jüngst reformierten Telekompakets ist, bestimmte Vorschriften und Verfahren zur Begrenzung von Urheberrechtsverletzungen in kleinem Maßstab durch Verbraucher beinhaltet ([31]). Zu diesen Verfahren gehört die Verpflichtung durch die Mitgliedstaaten, standardisierte Informationen von öffentlichem Interesse zu verschiedenen Themen, insbesondere zu Verstößen gegen das Urheberrecht und verwandte Schutzrechte und ihre rechtlichen Folgen, zu erstellen ([32]). Die Mitgliedstaaten können dann von den Internet-Diensteanbietern verlangen, diese Informationen an alle ihre Kunden weiterzugeben und in ihre Verträge aufzunehmen.

38. Mit dem System sollen natürliche Personen unterrichtet und von der Weitergabe urheberrechtlich geschützter Informationen sowie von der Beteiligung an Rechtsverletzungen abgehalten werden, während zugleich eine Überwachung der Internetnutzung und die damit verbundenen Bedenken in Bezug auf Privatsphäre und Datenschutz vermieden werden. Die Richtlinie „Rechte der Bürger" muss bis Mai 2011 umgesetzt werden; derartige Verfahren sind somit derzeit noch nicht vorhanden. Daher gab es bisher noch nicht die Möglichkeit, ihre Vorteile zu erproben. Es erscheint somit voreilig, die potenziellen positiven Ergebnisse dieser neuen Verfahren unberücksichtigt zu lassen und stattdessen „Three-Strikes-Internetsperren" einzuführen, die eine viel stärkere Beschränkung der Grundrechte nach sich ziehen.

39. Außerdem sei daran erinnert, dass Richtlinie 2004/48/EG vom 28. April 2004 zur Durchsetzung von Rechten des geistigen Eigentums diverse Instrumente zur Durchsetzung von Rechten des geistigen Eigentums vor Gericht vorsieht (Erörterung in Randnummern 43 ff.) ([33]).

40. Die Richtlinie zum geistigen Eigentum wurde erst kürzlich in das einzelstaatliche Recht der Mitgliedstaaten umgesetzt. Die Zeit reicht noch nicht aus, um zu beurteilen, ob sich ihre Bestimmungen für die Zwecke der Durchsetzung von Rechten des geistigen Eigentums eignen. Daher ist eine eventuelle Notwendigkeit, das auf Gerichtsverfahren basierende derzeitige System, das bis jetzt noch nicht erprobt wurde, zu ersetzen, zumindest fraglich. Die vorstehenden Ausführungen werfen unvermeidlicherweise die Frage auf, warum vorliegende Verstöße nicht mit den bestehenden zivil- und strafrechtlichen Instrumenten für Urheberrechtsverletzungen geahndet werden können. Dementsprechend sollte die Kommission, bevor derartige politische Maßnahmen vorgeschlagen werden, zuverlässige Informationen generieren, mit denen nachgewiesen werden kann, dass der derzeitige Rechtsrahmen nicht zu den beabsichtigten Wirkungen geführt hat.

41. Zudem ist unklar, ob ernsthaft über alternative, wirtschaftliche Geschäftsmodelle nachgedacht wurde, die keine systematische Überwachung natürlicher Personen implizieren. Wenn Urheberrechtsinhaber ihre Verluste aufgrund der Nutzung von P2P-Netzwerken nachweisen, könnten sie beispielsweise zusammen mit Internet-Diensteanbietern differenzierte Verträge für den Internetzugang erproben, bei denen ein Teil der Gebühr für einen unbeschränkten Zugang an die Urheberrechtsinhaber abgeführt wird.

Die Möglichkeit, eine gezielte Überwachung in einer Weise durchzuführen, die weniger starke Eingriffe nach sich zieht

42. Neben dem Einsatz vollständig anderer Modelle, die — wie oben dargelegt — geprüft und erprobt werden sollten, könnte eine gezielte Überwachung auf jeden Fall auf eine Weise erfolgen, die weniger starke Eingriffe mit sich bringt.

43. Der Zweck der Durchsetzung von Rechten des geistigen Eigentums kann auch erreicht werden, indem nur eine begrenzte Zahl von natürlichen Personen überwacht wird, bei denen der Verdacht der Beteiligung an nicht trivialen Verstößen gegen das Urheberrecht besteht. Die Richtlinie zum geistigen Eigentum enthält diesbezüglich gewisse Leitlinien. Sie legt die Bedingungen fest, unter denen Behörden anordnen können, dass im Besitz von Internet-Zugangsanbietern befindliche personenbezogene Daten für die Zwecke der Durchsetzung von Rechten des geistigen Eigentums offenzulegen sind. Nach Artikel 8 können die zuständigen Gerichte im Falle von Rechtsverletzungen *in gewerblichem Ausmaß* auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag hin anordnen, dass die Internet-Diensteanbieter in ihrem Besitz befindliche personenbezogene Informationen über mutmaßliche Rechtsverletzer (z.B. Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen) erteilen ([34]).

44. Dementsprechend ist das Kriterium des „gewerblichen Ausmaßes" entscheidend. Diesem Kriterium zufolge kann im Kontext von begrenzten, spezifischen *Ad-hoc*-Situationen, in denen wohlbegründete Verdachtsmomente für einen Urheberrechtsmissbrauch in gewerblichem Ausmaß vorliegen,

([31]) Siehe Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. L 337 vom 18.12.2009, S. 11.

([32]) Artikel 21 Absatz 4 der Richtlinie 2009/136/EG besagt insbesondere: „Die Mitgliedstaaten können verlangen, dass die in Absatz 3 genannten Unternehmen erforderlichenfalls Informationen von öffentlichem Interesse kostenlos über dieselben Hilfsmittel, über die sie gewöhnlich mit Teilnehmern kommunizieren, an bestehende und neue Teilnehmer weitergeben. Die betreffenden Informationen werden in einem solchen Fall von den zuständigen öffentlichen Behörden in einem standardisierten Format geliefert und erstrecken sich unter anderem auf folgende Themen: a) die häufigsten Formen einer Nutzung elektronischer Kommunikationsdienste für unrechtmäßige Handlungen oder die Verbreitung schädlicher Inhalte, insbesondere wenn dadurch die Achtung der Rechte und Freiheiten anderer Personen beeinträchtigt werden kann, einschließlich Verstößen gegen das Urheberrecht und verwandte Schutzrechte und ihre rechtlichen Folgen (…)." Artikel 20 Absatz 1 besagt überdies: „Die Mitgliedstaaten können ferner verlangen, dass der Vertrag auch die von den zuständigen öffentlichen Behörden gegebenenfalls zu diesem Zweck bereitgestellten Informationen nach Artikel 21 Absatz 4 über die Nutzung elektronischer Kommunikationsnetze und -dienste für unrechtmäßige Handlungen oder die Verbreitung schädlicher Inhalte und über die Möglichkeiten des Schutzes vor einer Gefährdung der persönlichen Sicherheit, der Privatsphäre und personenbezogener Daten enthält, die für den angebotenen Dienst von Bedeutung sind."

([33]) ABl. L 157 vom 30.4.2004, S. 45. (nachstehend „Richtlinie zum geistigen Eigentum").

([34]) Dies wird in Erwägungsgrund 14 der Richtlinie zum geistigen Eigentum weiter bestätigt.

eine Überwachung verhältnismäßig sein. Dieses Kriterium würde Situationen eines eindeutigen Urheberrechtsmissbrauchs durch Privatpersonen mit dem Ziel der Erlangung unmittelbarer oder mittelbarer wirtschaftlicher und gewerblicher Vorteile umfassen.

45. Um diese Bestimmung wirksam zu machen, könnten Urheberrechtsinhaber in der Praxis eine gezielte Überwachung bestimmter IP-Adressen vornehmen, um das Ausmaß der Urheberrechtsverletzung zu verifizieren. Dies würde bedeuten, dass es Urheberrechtsinhabern auch gestattet wäre, zu diesen Zwecken Meldungen über angebliche Rechtsverletzungen nachzugehen. Derartige Informationen sollten erst verwendet werden, nachdem die Signifikanz der Rechtsverletzung verifiziert wurde. Dazu gehören beispielsweise eindeutige Fälle erheblicher Rechtsverletzungen sowie geringfügige, aber fortlaufende Rechtsverletzungen über einen gewissen Zeitraum mit dem Ziel eines gewerblichen Vorteils oder eines finanziellen Gewinns. Das Erfordernis der Fortdauer über gewisse Zeiträume wird betont und in der Erörterung im Zusammenhang mit dem Grundsatz der Aufbewahrung weiter unten eingehender erläutert.

46. Dies bedeutet, dass in solchen Fällen die Erhebung von Informationen für den Zweck des Nachweises eines mutmaßlichen Internetmissbrauchs für die Vorbereitung gerichtlicher Schritte, einschließlich eines Prozesses, als verhältnismäßig und notwendig gelten kann.

47. Der EDSB ist der Auffassung, dass die Datenverarbeitungen, die auf die Erhebung dieser Art von Beweismitteln abzielen, als zusätzliche Sicherheit vorab durch die einzelstaatlichen Datenschutzstellen geprüft und genehmigt werden sollten. Diese Einschätzung basiert auf der Tatsache, dass die Datenverarbeitungen in Anbetracht ihrer Ziele, d.h. der Ausführung von Durchsetzungsmaßnahmen, die letztendlich rechtswidrig sein könnten, und unter Berücksichtigung des sensiblen Charakters der erhobenen Daten, spezifische Risiken für die Rechte und Freiheiten natürlicher Personen darstellen. Die Tatsache, dass die Verarbeitung eine Überwachung der elektronischen Kommunikation umfasst, ist ein zusätzlicher Faktor, der eine verstärkte Aufsicht erforderlich macht.

48. Nach Ansicht des EDSB ist das in der Richtlinie zum geistigen Eigentum verankerte „gewerbliche Ausmaß" ein äußerst geeignetes Element für die Festlegung der Grenzen der Überwachung, um den Grundsatz der Verhältnismäßigkeit zu wahren. Zudem scheint es keine zuverlässigen Belege dafür zu geben, dass sich gerichtliche Schritte gegen Urheberrechtsverletzer gemäß den Kriterien der Richtlinie zum geistigen Eigentum als nicht möglich oder unwirksam erweisen. Vielmehr scheinen Berichte — beispielsweise aus Deutschland, wo seit dem Jahr 2008, nach der Umsetzung der Richtlinie zum geistigen Eigentum, etwa 3 000 gerichtliche Verfügungen ergangen sind, denen zufolge Internet-Diensteanbieter den Gerichten gegenüber die Teilnehmerdaten von 300 000 Teilnehmern offengelegt haben — das Gegenteil nahezulegen.

49. Kurz gesagt: Da die Richtlinie zum geistigen Eigentum erst seit zwei Jahren in Kraft ist, ist schwer zu verstehen, warum Gesetzgeber von den in dieser Richtlinie verankerten Kriterien zu Methoden übergehen sollten, die stärkere Eingriffe darstellen, wenn die EU gerade erst beginnt, diese vor Kurzem eingeführten Methoden zu erproben. Schwer zu verstehen ist aus demselben Grund auch die Notwendigkeit, das derzeitige gerichtsbasierte System durch eine andere Art von Maßnahmen zu ersetzen (wodurch überdies Fragen in Bezug auf die Rechtsstaatlichkeit aufgeworfen werden, die hier nicht behandelt werden).

IV.4 **Übereinstimmung von Three-Strikes-Internetsperren mit detaillierteren Datenschutzbestimmungen**

50. Es gibt weitere, spezifischere rechtliche Gründe dafür, dass das Three-Strikes-Konzept aus datenschutzrechtlicher Sicht problematisch ist. Der EDSB möchte den rechtlichen Grund für die Verarbeitung, der durch Richtlinie 95/46/EG verlangt wird, und die in Richtlinie 2002/58/EG enthaltene Verpflichtung zur Löschung von Protokolldateien hervorheben.

Rechtlicher Grund für die Verarbeitung

51. Three-Strikes-Regelungen ziehen die Verarbeitung personenbezogener Daten nach sich, die zum Teil für Gerichts- oder Verwaltungsverfahren verwendet werden, mit denen das Ziel verfolgt wird, wiederholten Rechtsverletzern den Internetzugang zu sperren. Unter diesem Gesichtspunkt sind solche Daten als sensible Daten im Sinne von Artikel 8 der Richtlinie 95/46/EG einzustufen. Artikel 8 Absatz 5 besagt: „Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen …"

52. In diesem Kontext ist an das bereits erwähnte Arbeitspapier der Artikel-29-Datenschutzgruppe zu erinnern, in dem die Frage der Verarbeitung von Strafverfolgungsdaten erörtert wird ([35]). Die Gruppe erklärt Folgendes: „Wenngleich dem Einzelnen zweifelsohne das Recht zusteht, Strafverfolgungsdaten im Rahmen eines eigenen Rechtsstreits zu verarbeiten, so geht der Grundsatz doch nicht so weit, dass er die gründliche Ermittlung, Erfassung und Zentralisierung personenbezogener Daten durch Dritte erlauben würde, wozu auch generelle systematische Ermittlungen wie das Durchforsten des Internets (Internet-Scanning) zählen (…). Derartige Ermittlungen sind Sache der Strafverfolgungsbehörden" ([36]). Wenngleich — insbesondere in Fällen schwerer Verstöße — die Erhebung gezielter, spezifischer Beweismittel erforderlich sein mag, um einen Rechtsanspruch zu erhärten und auszuüben, teilt der EDSB voll und ganz die Auffassung der Artikel-29-Datenschutzgruppe hinsichtlich der fehlenden Legitimität großmaßstäblicher Ermittlungen, welche die Verarbeitung großer Mengen an Daten von Internetnutzern beinhalten.

53. Die Erörterung des oben beschriebenen Grundsatzes der Verhältnismäßigkeit und des Kriteriums des „gewerblichen Ausmaßes" sind relevant für die Ermittlung der Bedingungen für die Legitimierung der Erhebung von IP-Adressen und mit diesen verknüpften Informationen.

([35]) Siehe Randnummer 28 dieser Stellungnahme.
([36]) Hervorhebung hinzugefügt.

54. Internet-Diensteanbieter könnten versuchen, die von Urheberrechtsinhabern durchgeführte Verarbeitung zu legitimieren, indem sie Klauseln in die Verträge mit ihren Kunden aufnehmen, welche die Überwachung ihrer Daten und die Sperrung ihrer Zugänge gestatten. Dann würde davon ausgegangen werden, dass die Kunden mit dem Abschluss solcher Verträge in die Überwachung eingewilligt haben. Diese Vorgehensweise wirft jedoch zunächst die grundlegende Frage auf, ob natürliche Personen Internet-Diensteanbietern ihre Einwilligung zu einer Datenverarbeitung erteilen können, die nicht von dem Internet-Diensteanbieter durchgeführt wird, sondern von Dritten, die nicht der „Zuständigkeit" des Internet-Diensteanbieters unterstehen.

55. Zweitens stellt sich die Frage der Gültigkeit der Einwilligung. Artikel 2 Buchstabe h der Richtlinie 95/46/EG definiert Einwilligung als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden". Ein wichtiger Punkt ist, dass es sich gemäß der Begriffsbestimmung in Artikel 2 Buchstabe h der Richtlinie bei der Einwilligung, ungeachtet der Umstände, unter denen sie erteilt wird, um eine ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte Willensbekundung der betroffenen Person handeln muss, damit diese gültig ist. Der EDSB hat ernste Zweifel daran, dass die um ihre Einwilligung zu der Überwachung ihrer Internetaktivitäten ersuchten natürlichen Personen die Möglichkeit haben, eine wirkliche Entscheidung zu treffen — insbesondere aufgrund der Tatsache, dass die Alternative der Verzicht auf einen Internetzugang wäre, was möglicherweise viele andere Bereiche ihres Lebens beeinträchtigen würde.

56. Drittens ist äußerst fraglich, ob eine solche Überwachung jemals als für die Erfüllung eines Vertrags, den die betroffene Person als Vertragspartei geschlossen hat, *erforderlich* betrachtet werden könnte, wie dies durch Artikel 7 Buchstabe b der Richtlinie 95/46/EG vorgeschrieben wird, da die Überwachung offenkundig kein Gegenstand des von der betroffenen Person geschlossenen Vertrags ist, sondern nur ein anderen Interessen dienendes Mittel für den Internet-Diensteanbieter.

Löschung von Protokolldateien

57. Nach Richtlinie 2002/58/EG, insbesondere Artikel 6, dürfen Verkehrsdaten wie IP-Adressen nur aus unmittelbar mit der Kommunikation selbst verknüpften Gründen erhoben und gespeichert werden, worunter auch die Zwecke der Gebührenabrechnung, der Verkehrsabwicklung und der Betrugsverhütung fallen. Anschließend müssen die Daten gelöscht werden. Dies gilt unbeschadet der Verpflichtungen gemäß der Richtlinie über die Vorratsdatenspeicherung, die — wie erörtert — die Aufbewahrung von Verkehrsdaten und deren Offenlegung an Polizei- und Strafverfolgungsbehörden vorschreibt, um die Untersuchung **ausschließlich schwerer Straftaten** zu unterstützen ([37]).

([37]) Siehe Randnummer 35 dieser Stellungnahme.

58. In Übereinstimmung mit den oben dargelegten Bestimmungen sollten Internet-Diensteanbieter eventuelle Protokolldateien mit Informationen über die Aktivitäten von Internetnutzern, die für die oben genannten Zwecke nicht mehr benötigt werden, löschen. Unter Berücksichtigung der Tatsache, dass Protokolldateien für Abrechnungszwecke nicht erforderlich sind, sollten drei oder vier Wochen für die Verkehrsabwicklungszwecke des Internet-Diensteanbieters ausreichen ([38]).

59. Dies bedeutet, dass Internet-Diensteanbietern, die von Urheberrechtsinhabern kontaktiert werden (sofern diese Kontakte nicht innerhalb des oben dargelegten begrenzten Zeitraums erfolgen), die Protokolldateien, über die die IP-Adressen mit den jeweiligen Teilnehmern verknüpft sind, nicht vorliegen sollten. Die Aufbewahrung der Protokolldateien über diesen Zeitraum hinaus sollte nur in wohlbegründeten Fällen und innerhalb des Anwendungsbereichs der gesetzlich vorgesehenen Zwecke erfolgen.

60. In der Praxis bedeutet dies, dass den an Internet-Diensteanbieter gerichteten Ersuchen von Urheberrechtsinhabern — sofern diese nicht sehr schnell übermittelt werden — einfach aus dem Grund nicht nachgekommen werden kann, dass den Internet-Diensteanbietern die Informationen nicht mehr vorliegen. Dies allein legt die Grenzen dessen fest, was unter den im vorigen Abschnitt beschriebenen, akzeptablen Überwachungspraktiken zu verstehen ist.

Risiken von Ausstrahlungseffekten

61. Der EDSB hat nicht nur Bedenken hinsichtlich der Auswirkungen von Three-Strikes-Internetsperren in Bezug auf Privatsphäre und Datenschutz, sondern auch in Bezug auf ihre Ausstrahlungseffekte. Sollten Three-Strikes-Internetsperren erlaubt werden, könnten sie ein Dammbruchargument für eine noch massivere Überwachung der Aktivitäten von Internetnutzern sein, und zwar in unterschiedlichen Bereichen und für unterschiedliche Zwecke.

62. Der EDSB ersucht die Kommission dringend, dafür Sorge zu tragen, dass das ACTA nicht über das derzeitige EU-System für die Durchsetzung von Rechten des geistigen Eigentums, das die Grundrechte und -freiheiten sowie die Bürgerrechte, beispielsweise den Schutz personenbezogener Daten, achtet, hinausgeht und gegen dessen Bestimmungen verstößt.

V. DATENSCHUTZRECHTLICHE BEDENKEN IN BEZUG AUF MECHANISMEN DER INTERNATIONALEN ZUSAMMENARBEIT

63. Eines der von Teilnehmern an den ACTA-Verhandlungen vorgeschlagenen Mittel, um das Problem der Durchsetzung von Rechten des geistigen Eigentums zu lösen, ist die Stärkung der internationalen Zusammenarbeit durch eine Reihe

([38]) Die Verkehrsabwicklung umfasst die Analyse des Verkehrs in Computernetzwerken, um die Leistung zu optimieren oder sicherzustellen, die Latenzzeit zu senken und/oder die nutzbare Bandbreite zu erhöhen.

von Maßnahmen, die die wirksame Durchsetzung von Rechten des geistigen Eigentums in den Rechtssystemen der ACTA-Unterzeichnerstaaten ermöglichen würden.

64. In Anbetracht der verfügbaren Informationen ist absehbar, dass mehrere der zur Sicherstellung der Durchsetzung von Rechten des geistigen Eigentums vorgesehenen Maßnahmen die internationale, gemeinsame Nutzung von Informationen über mutmaßliche Verletzungen von Rechten des geistigen Eigentums durch Behörden (beispielsweise Zollbehörden, Polizei und Justiz), aber auch durch öffentliche und private Akteure (beispielsweise Internet-Diensteanbieter und Organisationen von Urheberrechtsinhabern) umfassen werden. Eine derartige Datenübermittlung wirft aus Sicht des Datenschutzes diverse Fragen auf.

V.1 **Ist der im Kontext des ACTA geplante Datenaustausch legitim, notwendig und verhältnismäßig?**

65. Beim derzeitigen Stand des Verhandlungsprozesses, bei dem eine Reihe konkreter Elemente im Bereich der Datenverarbeitung entweder noch nicht definiert oder aber unbekannt ist, lässt sich unmöglich verifizieren, ob der vorgeschlagene Rahmen von Maßnahmen den fundamentalen Datenschutzgrundsätzen und dem Datenschutzrecht der EU entspricht.

66. Zunächst ist zu bezweifeln, dass die Datenübermittlung in Drittländer im Kontext des ACTA legitim ist. Die Relevanz der Verabschiedung von Maßnahmen auf internationaler Ebene in diesem Bereich kann in Frage gestellt werden, solange es innerhalb der EU-Mitgliedstaaten keine Einigkeit in Bezug auf die Harmonisierung von Durchsetzungsmaßnahmen im digitalen Umfeld und die Art der anzuwendenden strafrechtlichen Sanktionen gibt ([39]).

67. In Anbetracht der obigen Ausführungen scheinen die Grundsätze der Notwendigkeit und Verhältnismäßigkeit von Datenübermittlungen im Rahmen des ACTA leichter erreichbar zu sein, wenn sich das Abkommen ausdrücklich auf die Bekämpfung der schwersten Vergehen im Bereich der Verletzung von Rechten des geistigen Eigentums beschränken würde, statt eine massenhafte Datenübermittlung im Zusammenhang mit allen mutmaßlichen Verletzungen von Rechten des geistigen Eigentums zu gestatten. Dies wird eine genaue Definition dessen erfordern, was „schwerste Vergehen im Bereich der Verletzung von Rechten des geistigen Eigentums" sind, bei denen eine Datenübermittlung erfolgen darf.

68. Überdies sollte den an dem Datenaustausch beteiligten Personen besondere Aufmerksamkeit gewidmet werden — ebenso wie der Frage, ob eine gemeinsame Nutzung von Daten nur zwischen Behörden erfolgen wird, oder ob diese auch einen Austausch zwischen privaten Akteuren und Behörden umfassen wird. Wie weiter oben in dieser Stellungnahme dargelegt wurde, gibt die Beteiligung privater Akteure in einem Bereich, der grundsätzlich der Zuständigkeit von Strafverfolgungsbehörden untersteht, Anlass zu einer Reihe von Bedenken ([40]). Die Bedingungen, unter denen private Akteure an der Erhebung von personenbezogenen Daten im Zusammenhang mit Verletzungen von Rechten des geistigen Eigentums sowie an deren Austausch mit Behörden beteiligt sind, sollten strikt auf besondere Umstände beschränkt und mit geeigneten Sicherheitsvorkehrungen verknüpft werden.

V.2 **Anwendbares Datenschutzrecht, das die Datenübermittlung im Kontext des ACTA regelt**

Allgemeine Regelungen für die Datenübermittlung

69. Der allgemeine, in der EU anwendbare Datenschutzrahmen wird durch Richtlinie 95/46/EG festgelegt. Die Artikel 25 und 26 der Richtlinie 95/46/EG definieren die für die Datenübermittlung in Drittländer anwendbaren Regelungen. Artikel 25 besagt, dass eine Übermittlung nur in Länder erfolgen darf, die ein angemessenes Schutzniveau gewährleisten; anderenfalls ist eine derartige Übermittlung grundsätzlich untersagt.

70. Die Angemessenheit des Schutzes personenbezogener Daten in Drittländern wird von der Europäischen Kommission auf Einzelfallbasis beurteilt; sie hat im Anschluss an eine eingehende Analyse der Artikel-29-Datenschutzgruppe mehrere Entscheidungen zur Anerkennung der Angemessenheit des Datenschutzniveaus bestimmter Länder erlassen ([41]).

71. Der EDSB merkt an, dass die meisten Teilnehmer an den ACTA-Verhandlungen nicht auf der von der Kommission erstellten Liste der ein angemessenes Datenschutzniveau bietenden Länder stehen: Abgesehen von der Schweiz und — unter bestimmten Umständen — Kanada und den Vereinigten Staaten verfügen alle anderen Teilnehmer an den ACTA-Verhandlungen nicht über die Anerkennung der Angemessenheit ihres Schutzniveaus. Dies bedeutet, dass für die Übermittlung von Daten aus der EU in eines dieser Länder eine der Bedingungen von Artikel 26 Absatz 1 der Richtlinie 95/46/EG erfüllt sein muss, oder dass die Parteien der Datenübermittlung angemessene Garantien im Sinne von Artikel 26 Absatz 2 der Richtlinie bieten müssen.

Sonderregelung für Datenübermittlungen im Bereich der Strafverfolgung

72. Die Richtlinie 95/46/EG stellt zwar das wichtigste Datenschutzinstrument in der EU dar, ihr Anwendungsbereich ist jedoch derzeit begrenzt, da sie ausdrücklich (unter anderem) die Tätigkeiten des Staates im strafrechtlichen Bereich ausschließt (Artikel 3). Der Datenaustausch für Strafverfolgungszwecke fällt somit nicht in den Anwendungsbereich

([39]) Ein Vorschlag zu strafrechtlichen Sanktionen wird derzeit im Rat erörtert, KOM(2006) 168 vom 26. April 2006.

([40]) Siehe Randnummern 32 und 52 dieser Stellungnahme. Siehe auch die Stellungnahme des EDSB vom 11. November 2008 zu dem Abschlussbericht der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten, ABl. C 128 vom 6.6.2009, S. 1.

([41]) Siehe Angemessenheitsentscheidungen der Europäischen Kommission in Bezug auf Argentinien, Kanada, die Schweiz, USA „Sicherer Hafen" und US-Behörden im Kontext der Übermittlung von Fluggastdatensätzen (PNR), Guernsey, Insel Man, und Jersey; abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm

der Richtlinie 95/46/EG, sondern unterliegt den allgemeinen Datenschutzgrundsätzen gemäß dem Übereinkommen Nr. 108 des Europarates und dessen Zusatzprotokoll, die von allen Mitgliedstaaten der EU ratifiziert wurden ([42]). Überdies gelten die von der EU angenommenen Vorschriften bezüglich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, die im Rahmenbeschluss 2008/877/JI des Rates festgelegt sind ([43]).

73. Auch diese Instrumente stellen den Grundsatz auf, dass in dem Drittland, in das Daten übermittelt werden sollen, ein angemessenes Datenschutzniveau gegeben sein muss. Dabei sind mehrere Ausnahmen vorgesehen, insbesondere in Fällen, in denen das Drittland angemessene Garantien bietet. Ähnlich wie beim Datenaustausch gemäß Richtlinie 95/46/EG erfordert ein Datenaustausch im Bereich der Strafverfolgung daher, dass zwischen den Parteien der Datenübermittlung angemessene Garantien geboten werden, damit eine solche Übermittlung stattfinden kann.

Hin zu einer neuen Regelung für die Übermittlung von Daten

74. Für die nahe Zukunft ist die Annahme neuer, für alle Tätigkeitsbereiche der EU geltender gemeinsamer Vorschriften für den Datenschutz auf der Grundlage von Artikel 16 AEUV zu erwarten. Dies bedeutet, dass es in einigen Jahren möglicherweise einen umfassenden EU-Datenschutzrahmen geben wird, der für alle Tätigkeitsbereiche der EU kohärente Datenschutzvorschriften festlegen wird, die für alle Datenverarbeitungstätigkeiten ein einheitliches Niveau in Bezug auf Garantien und Sicherheitsvorkehrungen vorschreiben werden. Wie von Viviane Reding ([44]), Kommissionsmitglied für Justiz, Grund- und Bürgerrechte, ausgeführt wurde, soll dieser neue Rahmen als einheitliches, „modernes und umfassendes Rechtsinstrument" für den Datenschutz in der EU fungieren. Ein solcher Rahmen ist besonders willkommen, da er mehr Klarheit und Kohärenz in Bezug auf die in der EU für den Datenschutz geltenden Vorschriften bringen würde.

75. Im internationalen Kontext weist der EDSB auch auf die kürzlich von Datenschutzbehörden angenommene *Resolution on International standards for the protection of personal data and privacy* (Entschließung zu internationalen Standards für den Schutz personenbezogener Daten und der Privatsphäre) hin, die ein erster Schritt in Richtung der Festlegung globaler Datenschutzstandards ist ([45]). Die internationalen Standards umfassen eine Reihe von Datenschutzgarantien, die denjenigen der Richtlinie 95/46/EG und des Übereinkommens Nr. 108 ähnlich sind. Obgleich die internationalen Standards noch nicht verbindlich sind, bieten sie durchaus hilfreiche Leitlinien für die Datenschutzgrundsätze, die von Drittländern auf freiwilliger Basis angewandt werden können, um ihren Rechtsrahmen mit den Standards der EU vereinbar zu machen. Nach Ansicht des EDSB sollten die Unterzeichner des ACTA auch die in den internationalen Standards für die Verarbeitung personenbezogener Daten aus der EU festgelegten Grundsätze berücksichtigen.

V.3 **Notwendigkeit der Einführung angemessener Garantien für den Schutz von Datenübermittlungen aus der EU in Drittländer**

Welche Form sollen die Garantien haben, um Datenübermittlungen in Drittländer wirksam zu schützen?

76. Wenn die Notwendigkeit einer Übermittlung personenbezogener Daten in Drittländer nachgewiesen ist, sollte die Europäische Union, wie der EDSB betont, mit Empfängern in Drittländern — zusätzlich zum ACTA selbst — spezifische Übereinkünfte aushandeln, die angemessene Datenschutzgarantien für die Regelung des Austauschs personenbezogener Daten enthalten.

77. Geeignete Datenschutzgarantien sollten üblicherweise in einem bindenden Abkommen zwischen der EU und dem Empfänger in dem jeweiligen Drittland festgelegt werden, durch das sich die empfangende Partei verpflichtet, das EU-Datenschutzrecht zu achten und natürliche Personen mit denselben Rechten und Rechtsmitteln auszustatten, wie sie nach EU-Recht gewährt werden. Die Notwendigkeit eines bindenden Abkommens geht aus Artikel 26 Absatz 2 der Richtlinie 95/46/EG und Artikel 13 Absatz 3 Buchstabe b des Rahmenbeschlusses hervor und wird überdies durch die bestehende Praxis der EU gestützt, spezifische Abkommen zu schließen, um spezifische Datenübermittlungen in Drittländer zu ermöglichen ([46]).

78. In ähnlicher Weise muss der Empfänger gemäß dem Entwurf der internationalen Standards möglicherweise garantieren, dass er das erforderliche Schutzniveau bieten wird, damit die Übermittlung erfolgen kann. Diese Garantien könnten ebenfalls die Form einer vertraglichen Zusage annehmen.

Inhalt der von Unterzeichnern des ACTA zu bietenden Garantien in Bezug auf die Übermittlung personenbezogener Daten

79. Der EDSB betont insbesondere, dass der internationale Austausch von Informationen für Strafverfolgungszwecke aus Datenschutzsicht besonders sensibel ist, da ein solcher Rahmen massenhafte Datenübermittlungen in einem Bereich

([42]) Übereinkommen des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, angenommen in Straßburg am 28. Januar 1981, und Europarat, Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, Straßburg, 8. November 2001.

([43]) Rahmenbeschluss 2008/877/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12. 2008, S. 60.

([44]) Siehe Antworten auf die Fragen des Europäischen Parlaments an das designierte Kommissionsmitglied Viviane Reding, S.5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_de.pdf

([45]) Entschließung angenommen im November 2009 in Madrid.

([46]) Beispielsweise Abkommen von Europol und Eurojust mit den Vereinigten Staaten, PNR-Abkommen, Swift-Abkommen, Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) aus der Europäischen Union und deren Übermittlung durch die Fluggesellschaften an die australische Zollbehörde.

legitimieren könnte, in dem die Auswirkungen auf natürliche Personen besonders schwer sind und in dem strikte und zuverlässige Garantien umso mehr erforderlich sind.

80. Der EDSB legt dar, dass spezifische Bedingungen und Garantien nur auf Einzelfallbasis und unter Berücksichtigung aller Parameter des jeweiligen Datenaustauschs festgelegt werden können. Als Orientierungshilfe zeigt der EDSB jedoch nachstehend einige der Grundsätze und Garantien auf, die von Empfängern in Drittländern geboten werden müssen, damit eine Übermittlung von Daten erfolgen kann:

— Es muss verifiziert werden, mit welcher rechtlichen Begründung die Datenverarbeitungstätigkeiten erfolgen (das heißt, basieren die Datenverarbeitungen auf einer gesetzlichen Verpflichtung, auf der Einwilligung seitens der betroffenen Personen oder auf einer anderen gültigen Begründung?), und ob bei der Datenübermittlung der anfängliche Zweck der Datenerhebung gewahrt wird. Außerhalb des Anwendungsbereichs des spezifizierten Zweckes sollte keine Übermittlung erfolgen.

— Die Menge und Art der auszutauschenden personenbezogenen Daten sollte eindeutig spezifiziert und auf das für die Erreichung des Zweckes der Übermittlung unbedingt erforderliche Mindestmaß beschränkt werden. Die erhobenen und übermittelten personenbezogenen Daten können insbesondere die IP-Adresse von Internetnutzern, Datum und Uhrzeit des mutmaßlichen Vergehens sowie die Art des Vergehens beinhalten. Der EDSB empfiehlt, dass Daten während der Ermittlungsphase nicht mit einer bestimmten Person verknüpft werden sollten, und erinnert daran, dass die Identifizierung einer verdächtigen Person nur in Übereinstimmung mit dem Gesetz erfolgen und der Kontrolle eines Richters unterliegen sollte. Dementsprechend legt der EDSB dar, dass Daten über Verletzungen von Rechten des geistigen Eigentums und mutmaßliche Rechtsverletzungen eine besondere Kategorie von Daten darstellen, deren Verarbeitung üblicherweise Strafverfolgungsbehörden vorbehalten ist und die Anwendung zusätzlicher Garantien erfordert. Die zur Verarbeitung von Daten über Verletzungen von Rechten des geistigen Eigentums und mutmaßliche Rechtsverletzungen befugten Personen und die Bedingungen für die Verarbeitung dieser Daten müssen daher in Übereinstimmung mit dem bestehenden Datenschutzrecht speziell festgelegt werden.

— Die Personen, zwischen denen die gemeinsame Nutzung der Daten erlaubt ist, müssen eindeutig festgelegt werden, und die Weiterübermittlung an andere Empfänger sollte grundsätzlich untersagt sein, sofern eine Weiterübermittlung nicht für eine spezifische Untersuchung erforderlich ist. Diese Begrenzung ist besonders wichtig, da die benannten Empfänger Informationen nicht unberechtigterweise gemeinsam mit nicht befugten Empfängern nutzen sollten.

— Der EDSB vermutet, dass das ACTA nicht nur eine Zusammenarbeit zwischen Behörden vorsehen wird, sondern dass es auch privaten Organisationen (beispielsweise Internet-Diensteanbietern und Organisationen von Urheberrechtsinhabern usw.) Durchsetzungsaufgaben übertragen wird. Im letztgenannten Fall müssen die Bedingungen für die und der Grad der Einbindung privater Organisationen in die Durchsetzung von Rechten des geistigen Eigentums sorgfältig beurteilt werden, und zwar unter der Maßgabe, dass ACTA-Maßnahmen Internet-Diensteanbietern und Organisationen von Urheberrechtsinhabern nicht *de facto* das Recht zur Überwachung des Online-Verhaltens von Nutzern verleihen sollten. Zudem sollte die Verarbeitung personenbezogener Daten durch private Organisationen im Kontext der Strafverfolgung nur auf einer angemessenen Rechtsgrundlage erfolgen. Ferner müssen auch eine eventuelle Verpflichtung privater Organisationen zur Zusammenarbeit mit der Polizei sowie das Ausmaß einer solchen Zusammenarbeit geklärt werden. Diese sollte auf jeden Fall ausschließlich auf „schwere Straftaten" beschränkt werden, wobei die Definition dieses Begriffs ebenfalls präzise festgelegt werden muss, weil nicht alle Verletzungen von Rechten des geistigen Eigentums als schwere Straftaten zu betrachten sind.

— Es muss auch eindeutig über die für den Austausch personenbezogener Daten zu verwendende Methode entschieden werden, wobei insbesondere spezifiziert werden sollte, ob dabei ein Push-System — zum Beispiel Übermittlung einer Reihe von Daten durch Internet-Diensteanbieter und Organisationen von Urheberrechtsinhabern unter eigener Kontrolle an Dritte (beispielsweise Polizei- und Strafverfolgungsbehörden) im Ausland — oder ein Pull-System — zum Beispiel unmittelbarer Zugriff von Polizei- und Strafverfolgungsbehörden auf Datenbanken Dritter oder auf Datenbanken, in denen Informationen zentralisiert werden — zur Anwendung kommen wird. Wie bereits im Kontext der Übermittlung von Fluggastdatensätzen (PNR) dargelegt wurde, ist ein Push-System die aus EU-Datenschutzsicht einzige Option, die mit den Datenschutzgrundsätzen vereinbar ist, da sie den Übermittler in der EU, bei dem es sich höchstwahrscheinlich um den für die Verarbeitung Verantwortlichen handelt, berechtigt, die Kontrolle über die Übermittlung von Daten auszuüben ([47]).

— Die Zeitspanne, während der eine Vorratsspeicherung personenbezogener Daten durch die Empfänger erfolgt, muss ebenso spezifiziert werden wie der Zweck, für den eine solche Vorratsspeicherung erforderlich ist. Der Zeitraum für eine solche Vorratsspeicherung sollte bezogen auf den zu erreichenden Zweck verhältnismäßig sein, was bedeutet, dass Daten gelöscht werden sollten, wenn sie für die Erreichung dieses Zweckes nicht mehr benötigt werden.

— Die Verpflichtungen, die für die Verarbeitung Verantwortlichen in Drittländern auferlegt werden, sollten eindeutig festgelegt werden. Es müssen Aufsichtsmechanismen und/oder durchsetzbare Haftungsmechanismen garantiert werden, sodass im Falle einer unrechtmäßigen Verarbeitung oder sonstiger relevanter Zwischenfälle wirksame Rückgriffsrechte und Sanktionen gegen für die Verarbeitung Verantwortliche zur Verfügung stehen. Überdies sollten Rechtsbehelfsmechanismen eingeführt

([47]) Siehe *Article 29 Working Party Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data* (Stellungnahme 4/2003 der Artikel-29-Datenschutzgruppe zu dem in den USA gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdaten), WP78, 13. Juni 2003.

werden, damit natürliche Personen Beschwerde bei einer unabhängigen Datenschutzbehörde erheben und bei einem unabhängigen und unparteiischen Gericht wirksam Rechtsmittel einlegen können ([48]).

— Die zwischen den Parteien getroffene Übereinkunft sollte eindeutige Angaben zu den Rechten von betroffenen Personen in Bezug auf ihre personenbezogenen Daten enthalten, wenn diese Daten durch einen Empfänger in einem Drittland verarbeitet werden, um so zu garantieren, dass den betroffenen Personen wirksame Mittel für die Durchsetzung ihrer Rechte im Zusammenhang mit einer im Ausland durchgeführten Verarbeitung zur Verfügung stehen.

— Des Weiteren ist Transparenz von entscheidender Bedeutung, und die Parteien der Datenschutzübereinkunft müssen sich darüber verständigen, wie sie betroffene Personen über die erfolgende Datenverarbeitung sowie über ihre Rechte und die Möglichkeiten der Ausübung dieser Rechte informieren werden.

VI. **FAZIT**

81. Der EDSB bestärkt die Europäische Kommission entschieden darin, einen öffentlichen und transparenten Dialog über das ACTA aufzunehmen, möglicherweise im Wege einer öffentlichen Konsultation; dies würde auch dazu beitragen, sicherzustellen, dass die zu erlassenden Maßnahmen den Anforderungen des EU-Rechts im Bereich der Privatsphäre und des Datenschutzes entsprechen.

82. Der EDSB appelliert eindringlich an die Europäische Kommission, im Zuge der laufenden Verhandlungen über das ACTA den richtigen Mittelweg zwischen den Forderungen nach Schutz von Rechten des geistigen Eigentums und dem Recht auf Schutz der Privatsphäre und auf Datenschutz zu finden. Der EDSB betont, dass es von besonderer Bedeutung ist, dass Privatsphäre und Datenschutz von Beginn der Verhandlungen an berücksichtigt werden, bevor eventuelle Maßnahmen vereinbart werden, damit nicht später alternative, dem Recht auf Privatsphäre gerecht werdende Lösungen gefunden werden müssen.

83. Obgleich das geistige Eigentum für die Gesellschaft wichtig ist und geschützt werden muss, sollte es nicht über die Grundrechte natürlicher Personen in Bezug auf Privatsphäre, Datenschutz und andere Rechte wie Unschuldsvermutung, effektiver Rechtsschutz und Meinungsfreiheit gestellt werden.

84. Insofern, als der derzeitige Entwurf des ACTA Three-Strikes-Internetsperren vorsieht oder zumindest auf derartige Maßnahmen drängt, würde das ACTA eine tief greifende Beschränkung der Grundrechte und -freiheiten europäischer Bürger beinhalten, insbesondere des Rechtes auf Schutz personenbezogener Daten und der Privatsphäre.

85. Der EDSB ist der Auffassung, dass Three-Strikes-Internetsperren nicht erforderlich sind, um den Zweck der Durchsetzung von Rechten des geistigen Eigentums zu erreichen. Der EDSB ist überzeugt, dass es alternative Lösungen gibt, die einen weniger starken Eingriff darstellen, oder dass die geplanten Sperren zumindest mit begrenzterem Umfang oder in einer Weise durchgeführt werden können, die einen weniger starken Eingriff darstellt, insbesondere in Form einer gezielten *Ad-hoc*-Überwachung.

86. Die Three-Strikes-Internetsperren sind auch auf detaillierterer rechtlicher Ebene problematisch, insbesondere aufgrund der Tatsache, dass die Verarbeitung von Strafverfolgungsdaten, vor allem durch private Organisationen, auf eine angemessene Rechtsgrundlage gestützt werden muss. Die Anwendung von Three-Strikes-Regelungen kann ferner die längerfristige Speicherung von Protokolldateien nach sich ziehen, was im Widerspruch zu geltenden Rechtsvorschriften stünde.

87. Da das ACTA den Austausch von personenbezogenen Daten zwischen Behörden und/oder privaten Organisationen mit Sitz in den Unterzeichnerstaaten beinhaltet, appelliert der EDSB zudem an die Europäische Union, angemessene Garantien einzuführen. Diese Garantien sollten für alle im Kontext des ACTA erfolgenden Datenübermittlungen gelten — unabhängig davon, ob sie im Rahmen der Strafverfolgung im zivilrechtlichen, strafrechtlichen oder digitalen Umfeld erfolgen — und sie sollten im Einklang mit den Datenschutzgrundsätzen des Übereinkommens Nr. 108 und der Richtlinie 95/46/EG stehen. Der EDSB empfiehlt, dass derartige Garantien die Form bindender Abkommen zwischen den Übermittlern in der EU und den Empfängern in Drittländern erhalten.

88. Der EDSB wünscht ferner, zu den im Zusammenhang mit den Datenübermittlungen im Rahmen des ACTA einzuführenden Maßnahmen angehört zu werden, um verifizieren zu können, dass diese verhältnismäßig sind und ein angemessenes Datenschutzniveau gewährleisten.

Geschehen zu Brüssel am 22. Februar 2010.

Peter HUSTINX

Europäischer Datenschutzbeauftragter

([48]) Siehe die Stellungnahme des EDSB zu dem Abschlussbericht der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten, 11.11.2008.