



Stellungnahme des Europäischen Datenschutzbeauftragten

zum Vorschlag für einen Beschluss des Rates über den Abschluss des Handelsübereinkommens zur Bekämpfung von Produkt- und Markenpiraterie zwischen der Europäischen Union und ihren Mitgliedstaaten, Australien, Kanada, Japan, der Republik Korea, den Vereinigten Mexikanischen Staaten, dem Königreich Marokko, Neuseeland, der Republik Singapur, der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika

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 7 und 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 Datenverkehr¹,

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 Datenverkehr², insbesondere Artikel 41 Absatz 2 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1.1. Der EU-Rechtsetzungsprozess zu ACTA

1. Am 24. Juni 2011 legte die Kommission einen Vorschlag für einen Beschluss des Rates über den Abschluss des Handelsübereinkommens zur Bekämpfung von Produkt- und Markenpiraterie zwischen der Europäischen Union und ihren Mitgliedstaaten, Australien, Kanada, Japan, der Republik Korea, den Vereinigten Mexikanischen Staaten, dem Königreich Marokko, Neuseeland, der Republik Singapur, der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika vor³.

¹ ABl. L 281 vom 23.11.1995, S. 31.

² ABl. L 8 vom 12.1.2001, S. 1.

³ Vorschlag der Kommission für einen Beschluss des Rates über den Abschluss des Handelsübereinkommens zur Bekämpfung von Produkt- und Markenpiraterie zwischen der Europäischen Union und ihren Mitgliedstaaten,

2. Ziel des Übereinkommens ist es, die Durchsetzung der Rechte des geistigen Eigentums durch die Entwicklung eines gemeinsamen Ansatzes zur Stärkung und Vereinfachung der Zusammenarbeit auf internationaler Ebene anzugehen. Kapitel II enthält Maßnahmen in verschiedenen Rechtsbereichen, insbesondere im Bereich der zivilrechtlichen Durchsetzung (Abschnitt 2), Grenzmaßnahmen (Abschnitt 3), strafrechtlichen Durchsetzung (Abschnitt 4) und der Durchsetzung der Rechte des geistigen Eigentums im digitalen Umfeld (Abschnitt 5). Kapitel III enthält Maßnahmen zur Verbesserung der Durchsetzungspraxis und in Kapitel IV wird auf die internationale Zusammenarbeit eingegangen.
3. ACTA wurde vom Rat im Dezember 2011⁴ einstimmig angenommen und von der Europäischen Kommission und 22 Mitgliedstaaten⁵ am 26. Januar 2012 unterzeichnet. Gemäß Artikel 40 des Übereinkommens wird ACTA nach Ratifizierung durch sechs der Unterzeichnerstaaten in Kraft treten. Um auf Unionsebene in Kraft zu treten, muss das Übereinkommen jedoch von der EU ratifiziert werden, was die Zustimmung des Europäischen Parlaments im Rahmen des Zustimmungsverfahrens für internationale Handelsübereinkommen⁶ und die Ratifizierung durch die Mitgliedstaaten im Rahmen ihrer jeweiligen verfassungsmäßigen Verfahren erforderlich macht. Die Abstimmung des Europäischen Parlaments über ACTA ist für 2012 im Rahmen einer Plenarsitzung vorgesehen.

1.2. Sachstand bezüglich ACTA in der EU

4. Während der letzten Monate wurde wachsende Besorgnis bezüglich ACTA⁷ zum Ausdruck gebracht. Dies veranlasste die Europäische Kommission dazu am 22. Februar 2012 ihre Absicht zu verkünden den Gerichtshof der Europäischen Union zu bitten ein Gutachten zum Handelsübereinkommens zu erarbeiten⁸. Ein solches Verfahren ist in Artikel 218 Absatz 11 des Vertrags über die Arbeitsweise der Europäischen Union („AEUV“)⁹ vorgesehen.
5. Am 4. April 2012 beschloss die Kommission, dem Gerichtshof folgende Frage zu unterbreiten: *„Ist das Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (ACTA) mit den Europäischen Verträgen, insbesondere mit der Charta*

Australien, Kanada, Japan, der Republik Korea, den Vereinigten Mexikanischen Staaten, dem Königreich Marokko, Neuseeland, der Republik Singapur, der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika, KOM(2011) 380 endgültig.

⁴ Die neueste Version des Textes des Übereinkommens des Rates vom 23. August 2011 ist verfügbar unter: <http://register.consilium.europa.eu/pdf/de/11/st12/st12196.de11.pdf>.

⁵ Deutschland, Zypern, Estland, die Niederlande und die Slowakei haben das Übereinkommen noch nicht unterzeichnet.

⁶ Gemäß Artikel 218 Absatz 6 AEUV.

⁷ Vgl. unter anderem: <http://euobserver.com/9/115043>; <http://euobserver.com/871/115128>; https://www.bfdi.bund.de/bfdi_forum/showthread.php?3062-ACTA-und-der-Datenschutz, <http://www.bbc.co.uk/news/technology-17012832>.

⁸ Erklärung von Kommissar Karel De Gucht zu ACTA (Handelsübereinkommen zur Bekämpfung der Produkt- und Markenpiraterie), <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/128>.

⁹ Artikel 218 Absatz 11 AEUV sieht Folgendes vor: „Ein Mitgliedstaat, das Europäische Parlament, der Rat oder die Kommission können ein Gutachten des Gerichtshofs über die Vereinbarkeit einer geplanten Übereinkunft mit den Verträgen einholen. Ist das Gutachten des Gerichtshofs ablehnend, so kann die geplante Übereinkunft nur in Kraft treten, wenn sie oder die Verträge geändert werden.“ Artikel 107 Absatz 2 der Verfahrensordnung des Gerichtshofs sieht Folgendes vor: „Das Gutachten kann sich sowohl auf die Vereinbarkeit des beabsichtigten Abkommens mit den Verträgen als auch auf die Zuständigkeit der Union oder eines ihrer Organe für den Abschluss eines solchen Abkommens erstrecken.“

der Grundrechte der Europäischen Union, vereinbar?“¹⁰ Im Falle eines negativen Bescheids sieht Artikel 218 Absatz 11 AEUV ganz eindeutig vor, dass „die geplante Übereinkunft nur in Kraft treten [kann], wenn sie oder die Verträge geändert werden“.

6. Der Verweis des Übereinkommens an den Gerichtshof durch die Kommission würde jedoch nicht automatisch zu einer Aussetzung des derzeit beim Europäischen Parlament anhängigen Zustimmungsverfahrens führen. Nach der Erörterung im Ausschuss für internationalen Handel des Europäischen Parlaments wurde beschlossen, mit der Abstimmung wie vorgesehen zu verfahren¹¹.

1.3. Die Gründe für eine zweite Stellungnahme des EDSB zu ACTA

7. Im Februar 2010 verfasste der EDSB auf eigene Initiative eine Stellungnahme, um die Kommission auf einige Aspekte aufmerksam zu machen, die den Schutz der Privatsphäre und den Datenschutz betreffen, die im Rahmen der ACTA-Verhandlungen berücksichtigt werden sollten¹². Obgleich die Verhandlungen vertraulich geführt wurden, gab es Hinweise darauf, dass ACTA Online-Durchsetzungsmaßnahmen enthalten würde, welche Auswirkungen auf die Datenschutzrechte haben würden, insbesondere die „Three-Strikes-Regelung“¹³.
8. Der EDSB konzentrierte sich zum damaligen Zeitpunkt in seiner Analyse auf die Rechtmäßigkeit und Verhältnismäßigkeit dieser Art von Maßnahmen und kam zu dem Schluss, dass die Aufnahme einer Maßnahme in ACTA, welche die massive Überwachung von Internet-Nutzern vorsieht, nicht mit den EU-Grundrechten und insbesondere den Rechten auf den Schutz der Privatsphäre und Datenschutz vereinbar wäre, die in Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 und 8 der Charta der Grundrechte der EU verankert sind¹⁴. Der EDSB unterstrich außerdem, welche Sicherheiten für den internationalen Austausch personenbezogener Daten im Kontext der Durchsetzung von Rechten des geistigen Eigentums erforderlich sind.
9. Nachdem nun der Text des Entwurfs des ACTA-Übereinkommens veröffentlicht wurde¹⁵, ist der EDSB der Ansicht, dass es angemessen ist, eine zweite ACTA-Stellungnahme zu verfassen, um einige der in der Übereinkunft enthaltenen Bestimmungen aus einer datenschutzrechtlichen Perspektive zu prüfen und dadurch spezifisches Fachwissen zur Verfügung zu stellen, das im Rahmen des Ratifizierungsverfahrens berücksichtigt werden könnte. Aus diesem Grund verfasste der EDSB gemäß Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 die vorliegende Stellungnahme in eigener Initiative, um Orientierungshilfen bezüglich der in ACTA zu berücksichtigenden Aspekte in den Bereichen des Schutzes der Privatsphäre und des Datenschutzes zu geben.

¹⁰ <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/354&format=HTML&aged=0&language=EN&guiLanguage=en>.

¹¹ Siehe <http://www.neurope.eu/article/parliament-halts-sending-acta-court-justice>.

¹² 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), ABl. C 147 vom 5.6.2010, S. 1.

¹³ „Three-Strikes-Internetsperren“ oder „graduated response“-Regelungen erlauben es Rechteinhabern oder beauftragten Dritten Internet-Nutzer zu überwachen und mutmaßliche Urheberrechtsverletzer zu identifizieren. Nachdem die Internet-Diensteanbieter über den mutmaßlichen Urheberrechtsverletzer informiert wurden, würden diese den identifizierten Nutzer verwarnen und nach drei Verwarnungen den Internetzugang sperren.

¹⁴ Charta der Grundrechte der Europäischen Union, ABl. C 303 vom 14.12.2007, S. 1.

¹⁵ Siehe Fußnote 3.

II. RAHMEN DER KOMMENTARE DES EDSB

10. Der EDSB erkennt das berechnigte Interesse an, die Durchsetzung der Rechte des geistigen Eigentums in einem internationalen Kontext sicherzustellen. Obgleich mehr internationale Zusammenarbeit zur Durchsetzung der Rechte des geistigen Eigentums erforderlich ist, dürfen die Mittel, die zur Stärkung der Rechtsdurchsetzung vorgesehen werden, nicht auf Kosten der Grundrechte natürlicher Personen gehen und insbesondere nicht auf Kosten ihrer Rechte auf Schutz der Privatsphäre und Datenschutz. Aus diesem Grund forderte der EDSB die Europäische Kommission zum Zeitpunkt der Verhandlungen auf, den richtigen Mittelweg zwischen den Forderungen nach Schutz von Rechten des geistigen Eigentums auf der einen Seite und dem Recht natürlicher Personen auf Schutz der Privatsphäre und auf Datenschutz auf der anderen Seite zu finden¹⁶. Die Notwendigkeit eines angemessenen Rechteaushleichs im Zusammenhang mit der Durchsetzung der Rechte des geistigen Eigentums wurde am 19. April 2012 auch vom Gerichtshof der Europäischen Union in der Rechtssache *Bonnier Audio AB*¹⁷ zum Ausdruck gebracht.
11. Wie nachfolgend weiter ausgeführt werden wird, stellt der EDSB fest, dass die Bestimmungen zur Durchsetzung der Rechte des geistigen Eigentums im Internet aus datenschutzrechtlicher Sicht Anlass zu Bedenken geben. Wie bereits erwähnt, wurde der Gerichtshof mit der Frage betraut, ob die ACTA-Bestimmungen mit den Europäischen Verträgen und insbesondere mit der Charta der Grundrechte vereinbar sind. Die Analyse im Rahmen dieser Stellungnahme befasst sich intensiver mit der Prüfung der Vereinbarkeit des Übereinkommens mit den EU-Bestimmungen zum Schutz der Privatsphäre und dem Datenschutz und prüft auch, ob die Bestimmungen des Übereinkommens, falls sie nicht korrekt umgesetzt werden, möglicherweise zu ungebührlichen und unannehmbaren Auswirkungen auf die Rechte natürlicher Personen auf den Schutz der Privatsphäre und den Datenschutz führen könnten. In anderen Worten: Enthält das Übereinkommen die richtigen Anreize dafür, dass die Gesetzgeber auf der Ebene der EU und der Mitgliedstaaten die Schutzbedürfnisse des Rechts auf Datenschutz berücksichtigen? Die vorliegende Stellungnahme sollte auf keinen Fall als Vorwegnahme des Gutachtens des Gerichtshofs verstanden werden.
12. Obgleich in dieser Stellungnahme hauptsächlich auf die Durchführungsmaßnahmen eingegangen wird, die im digitalen Kapitel des ACTA enthalten sind, werden – soweit von Belang – auch andere Bestimmungen des Übereinkommens geprüft. Die Stellungnahme baut auf der Analyse der früheren Stellungnahme des EDSB zu ACTA auf, die weiterhin uneingeschränkt gilt, im Hinblick auf die Gefahren etwaiger Maßnahmen zur Überwachung von Internet-Nutzern für die Privatsphäre und den Datenschutz und im Hinblick auf die Schutzmaßnahmen, die zum internationalen Austausch personenbezogener Daten im Kontext der Durchsetzung der Rechte des geistigen Eigentums erforderlich sind. Aus diesem Grund wird die frühere Analyse nicht vollständig wiederholt, es wird aber bei Bedarf darauf Bezug genommen. Nach Prüfung der Gefahren für die Privatsphäre und den Datenschutz der angestrebten Durchsetzungsmechanismen im digitalen Umfeld (Abschnitt III), wird insbesondere auf einige der Bestimmungen des Übereinkommens aus datenschutzrechtlicher Sicht eingegangen (Abschnitt IV).

¹⁶ Siehe Absatz 10 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

¹⁷ Vgl. Rechtssache C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB* gegen *Perfect Communication Sweden AB*, Urteil vom 19. April 2012.

III. GEFAHREN FÜR DEN DATENSCHUTZ UND DAS RECHT AUF PRIVATSPHÄRE DURCH DIE ANGESTREBTEN MASSNAHMEN ZUR DURCHSETZUNG IM DIGITALEN UMFELD

III.1. Im digitalen Kapitel des ACTA vorgesehene Maßnahmen (Kapitel II, Abschnitt 5)

13. Kapitel II Abschnitt 5 des ACTA enthält eine Reihe von Maßnahmen, die darauf abzielen, die Durchsetzung der Rechte des geistigen Eigentums im digitalen Umfeld zu erleichtern. Obgleich diese Maßnahmen darauf ausgerichtet sind, einen Beitrag zur Bekämpfung aller Formen der Rechtsverletzungen des geistigen Eigentums zu leisten, auch im Hinblick auf den Markenschutz, steht der Schutz von Urheberrechten im Mittelpunkt dieses Kapitels.
14. Das digitale Kapitel des ACTA enthält zwei Maßnahmen, die spezifisch darauf ausgerichtet sind, die Durchsetzung von Rechten des geistigen Eigentums im Online-Umfeld zu erleichtern. Diese Maßnahmen können von den Vertragsparteien umgesetzt werden, ohne dass die explizite Pflicht bestünde, diese in ihre Rechtsordnung aufzunehmen: (i) ein Mechanismus, durch den *„eine zuständige Behörde“* einem Online-Dienstanbieter anordnen kann, einem Rechteinhaber unverzüglich die nötigen Informationen zur Identifizierung eines verdächtigen Abonnenten offenzulegen¹⁸ und (ii) die Förderung von *„Kooperationsbemühungen im Wirtschaftsleben zu fördern, die darauf gerichtet sind, Verstöße gegen Marken, Urheberrechte oder verwandte Schutzrechte wirksam zu bekämpfen“*¹⁹.
15. Die erste Art von Maßnahme zielt darauf ab, die Offenlegung der Identität von Personen, deren Verhaltensweise auf Verstöße von Rechten am geistigen Eigentum im Online-Umfeld schließen lässt, an den Rechteinhaber sicherzustellen. Im Rahmen eines solchen Mechanismus wären Internetdiensteanbieter verpflichtet, personenbezogene Daten einiger ihrer Abonnenten gegenüber Rechteinhabern offenzulegen, sofern bestimmte Kriterien erfüllt sind und unter Aufsicht und Kontrolle einer Behörde.
16. Die zweite Art von Maßnahme ist weniger selbsterklärend als die Erste. Es ist nicht klar, welche Art von Maßnahme mit *„Kooperationsbemühungen im Wirtschaftsleben“* gemeint ist. Ein Erwägungsgrund der Präambel des ACTA ist konkreter und führt an, dass eine derartige Zusammenarbeit *„zwischen Dienstleistern und Rechteinhabern [wünschenswert ist], um einschlägigen Rechtsverletzungen im digitalen Umfeld entgegenzuwirken“*. Viele der Vertragsparteien, auf deren Gebiet bestimmte Arten freiwilliger Mechanismen der Zusammenarbeit zur Rechtsdurchsetzung bereits zwischen Internet-Diensteanbietern und Rechteinhabern umgesetzt wurden, werden vermutlich anführen, dass diese Mechanismen unter Artikel 27 Absatz 3 des Übereinkommens fallen. Dazu zählen verschiedene Formen der freiwilligen Mechanismen der Zusammenarbeit zur Rechtsdurchsetzung, wie die „Three-Strikes“-Mechanismen, das Sperren und Filtern des Peer-to-Peer-Datenverkehrs oder das Sperren von Webseiten, auf denen mutmaßlich Urheberrechtsverletzungen stattfinden.

¹⁸ Artikel 27 Absatz 4 des ACTA.

¹⁹ Artikel 27 Absatz 3 des ACTA.

III.2. Warum sind diese Mechanismen aus der Sicht des Datenschutzes auf EU-Ebene problematisch?

17. Das Internet erleichtert den Austausch von urheberrechtlich geschützten Inhalten auf unterschiedliche Weise²⁰; einiger dieser Aktivitäten bestehen im rechtmäßigen Austausch geschützter Werke, während andere sich auf unrechtmäßige Schaffung und Austausch von urheberrechtlich geschützten Inhalten beziehen. Von allen Rechten des geistiges Eigentums ist das Urheberrecht sicherlich dasjenige, dessen Durchsetzung im Internet mit den größten Herausforderungen und Bedenken im Hinblick auf den Schutz der Privatsphäre verbunden ist, insbesondere angesichts der großen Anzahl an Personen, die von Durchsetzungsmaßnahmen zum Schutz der Urheberrechte betroffen sein könnten die sich auf Online-Aktivitäten beziehen.
18. Viele der Maßnahmen, die im Kontext der Artikel 27 Absatz 3 und Artikel 27 Absatz 4 ACTA umgesetzt werden könnten, würden zu einer Form der Überwachung der Nutzung des Internets seitens natürlicher Personen führen, ganz gleich, ob diese darauf abzielen, effektive Verletzungen der Rechte des geistigen Eigentums aufzudecken oder zukünftige Rechtsverletzungen zu vermeiden. In vielen Fällen würde die Überwachung von den Rechteinhabern oder deren Verbänden bzw. beauftragten Dritten durchgeführt werden, obgleich häufig auch versucht wird, diese Aufgabe an die Internetdiensteanbieter zu delegieren²¹.
19. Maßnahmen, die eine generalisierte Überwachung der Tätigkeiten von Internetnutzern nach sich ziehen, stellen schwere Eingriffe in die Privatsphäre natürlicher Personen dar. Sie werden in der Regel unbemerkt durchgeführt und können Millionen natürlicher Personen oder sogar alle Nutzer betreffen, unabhängig davon, ob sie unter Verdacht stehen. Sie können die Überwachung der, über das Internet ausgetauschten, elektronischen Kommunikation mit sich bringen und die Überprüfung des Inhalts der Internetkommunikation natürlicher Personen, gesendeter und empfangener E-Mails, besuchter Webseiten, herunter- oder hochgeladener Dateien, etc. Des Weiteren bringt diese Überwachung in der Regel eine systematische Aufzeichnung von Daten mit sich, einschließlich der IP-Adressen der verdächtigen Nutzer. All diese Informationen können durch den Diensteanbieter mit einer bestimmten natürlichen Person verbunden werden, der den Abonnenten, dem die verdächtige IP-Adresse zugewiesen wurde, identifizieren kann. Dies sind folglich personenbezogene Daten gemäß der in Artikel 2 der Datenschutzrichtlinie 95/46/EG²² enthaltenen Definition.
20. Diese Maßnahmen stellen folglich häufig einen Eingriff in die Grundrechte und Freiheiten natürlicher Personen dar, wie die Rechte auf Schutz der Privatsphäre, Datenschutz und die Geheimhaltung von Mitteilungen, die in Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 und 8 der Charta der Grundrechte der EU verankert sind²³.
21. Die Rechtmäßigkeit spezifischer Durchsetzungsmaßnahmen, die Eingriffe in die Grundrechte und Freiheiten darstellen, müssen ausgehend von den in Artikel 8 Absatz 2

²⁰ Zum Beispiel über Peer-to-Peer-Netzwerke, über den Web-Download, Streaming, etc.

²¹ Dies gilt insbesondere im Hinblick auf die Vermeidung von Rechtsverletzungen, wobei Rechteinhaber beispielsweise von Internetdiensteanbietern fordern, dass diese Filterinstrumente zur Überwachung der Verhaltensweisen aller Nutzer im Internet einsetzen.

²² Vgl. Absatz 27 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

²³ Siehe Stellungnahme des EDSB vom 7. Oktober 2011 über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten, ABl. C 34 vom 8.2.2012, S. 1.

der Europäischen Menschenrechtskonvention²⁴ und Artikel 52 der Charta der Grundrechte der EU²⁵ enthaltenen Bestimmungen geprüft werden. Diese Bestimmungen sehen vor, dass jede Beschränkung gesetzlich vorgeschrieben und notwendig sein muss und in einem angemessenen Verhältnis zu den rechtmäßig verfolgten Zielen steht. Des Weiteren müssen die Maßnahmen, welche eine Verarbeitung personenbezogener Daten umfassen, mit den Datenschutzbestimmungen vereinbar sein, die unter anderem vorsehen, dass sie auf einer gültigen Rechtsgrundlage basieren.

22. Was die Notwendigkeit einer spezifischen Durchsetzungsmaßnahme angeht, die einen Eingriff in ein oder mehrere Grundrechte darstellt, muss zuerst der Nachweis dafür erbracht werden, dass diese Maßnahme einem dringenden Bedürfnis der Gesellschaft entspricht. Außerdem muss geprüft werden, ob andere, weniger einschneidende Alternativen zur Verfügung stehen oder denkbar sind²⁶.
23. Die Verhältnismäßigkeit einer spezifischen Durchsetzungsmaßnahme muss von Fall zu Fall und unter Berücksichtigung der Grundrechte geprüft werden mit denen diese kollidieren könnte. Um eine solche Bewertung vornehmen zu können, ist es erforderlich, dass die Maßnahme ausreichend präzise und klar definiert ist, um die konkrete Auswirkung auf die gemeinsame Nutzung von Daten sowie auf andere Grundrechte prüfen zu können²⁷. Des Weiteren muss die Maßnahme im Kontext der Durchsetzung von Rechten des geistigen Eigentums als Reaktion auf eine einzelne Rechtsverletzung angemessen sein; eine Maßnahme, die darauf abzielt, Verletzungen von Rechten des geistigen Eigentums generell zu vermeiden, wäre nicht verhältnismäßig.
24. Zwei Aspekte sind bei der Beurteilung der Verhältnismäßigkeit einer Maßnahme zur Durchsetzung von Rechten des geistigen Eigentums von besonderer Bedeutung: (i) die Größenordnung und die Tiefe der etwaigen Überwachung der Nutzung des Internets und der Internet-Nutzer und (ii) die Größenordnung der Verletzungen der Rechte des geistigen Eigentums, gegen welche eine derartige Maßnahme gerichtet ist.
25. Eine gezielte Form der Überwachung durch Rechteinhaber wäre legitim, wenn die Verarbeitung im Kontext spezifischer, laufender oder angestrebter Gerichtsverfahren durchgeführt wird, um Rechtsansprüche festzustellen, geltend zu machen oder zu verteidigen. Eine generalisierte Überwachung, auf welche dann eine generalisierte Speicherung der Daten zu Zwecken der Durchsetzung von Ansprüchen folgt, wie das Durchforsten des Internets (Internet-Scanning) oder der gesamten Tätigkeit in P2P-

²⁴ Artikel 8 Absatz 2 sieht Folgendes vor: „Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.“

²⁵ Artikel 52 Absatz 1 sieht Folgendes vor: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.“

²⁶ Vgl. Absatz 42 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

²⁷ Vgl. Gutachten des Generalanwalts Pedro Cruz Villalón, Rechtssache C-70/10, *Scarlet Extended SA gegen SABAM*, 14. April 2011, Randnummern 66 und 68.

Netzwerken, würde über das legitime Ziel hinausgehen. Eine derartige generalisierte Überwachung stellt insbesondere dann einen Eingriff in die Rechte und Freiheiten natürlicher Personen dar, wenn diese nicht gut definiert ist und keine Einschränkungen vorgesehen sind im Hinblick auf den Anwendungsbereich, den Zeitraum und die betroffenen Personen²⁸. Folglich wäre die wahllose oder ausgedehnte Überwachung der Verhaltensweisen von Internet-Nutzern im Zusammenhang mit unbedeutenden Rechtsverletzungen auf kleiner Skala, mit denen keine Gewinnabsicht verbunden ist, unangemessen und nicht mit Artikel 8 EMRK, den Artikeln 7 und 8 der Charta der Grundrechte und der Datenschutzrichtlinie vereinbar²⁹.

III.3. Der aktuelle EU-Rechtsrahmen

26. Aus Sicht der EU müssen die ACTA-Bestimmungen ausgehend von der aktuellen EU-Rechtsordnung zum Schutz der Grundrechte und dem Rechtsrahmen bezüglich der Durchsetzung von Rechten des geistigen Eigentums, dem Datenschutz sowie dem Haftungssystem von Internet-Vermittlern geprüft werden. Die im digitalen Kapitel des ACTA enthaltenen Durchsetzungsmaßnahmen unterliegen deshalb den Einschränkungen der EU-Rechtsordnung.
27. In der EU wurden die Grundrechte auf Schutz der Privatsphäre und Datenschutz im EU-Primärrecht in Artikel 16 AEUV und im EU-Sekundärrecht in der Richtlinie 95/46/EG und in der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG³⁰ weiter ausgearbeitet. Die Rechte auf Schutz der Privatsphäre und Datenschutz müssen außerdem ausgehend von der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte³¹ und des Gerichtshofs ausgelegt werden.
28. Der aktuelle EU-Rechtsrahmen zum Schutz der Rechte des geistigen Eigentums wurde sorgsam unter Berücksichtigung anderer Grundrechte, wie den Rechten auf Schutz der Privatsphäre und den Datenschutz, ausgearbeitet. Die Richtlinie zum geistigen Eigentum³² und in gewissem Maße die Richtlinie 2001/29/EG³³ legen gegenwärtig die Bedingungen für die Durchsetzung von Rechten des geistigen Eigentums in zivilrechtlichen Verfahren fest. Außerdem sollten die im ACTA vorgesehenen Durchsetzungsmaßnahmen auch mit der besonderen Haftungsregelung von Internetdiensteanbietern vereinbar sein, die in der Richtlinie über den elektronischen Geschäftsverkehr 2000/31/EG³⁴ enthalten ist und mit den Pflichten und

²⁸ Vgl. insbesondere Rechtssache C-70/10, *Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Urteil vom 24. November 2011, und Rechtssache C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) gegen Netlog NV*, Urteil vom 16. Februar 2012.

²⁹ Vgl. Absätze 31 bis 34 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

³⁰ 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.

³¹ Auslegung der wichtigsten Elemente und Bedingungen von Artikel 8 der am 4. November 1950 in Rom angenommenen Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten.

³² Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. L 195 vom 2.6.2004, S. 16.

³³ Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. L 167 vom 22.6.2001, S. 10–19.

³⁴ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl. L 178 vom 17.7.2000, S. 1.

Einschränkungen, denen die Internetdiensteanbieter gemäß der Richtlinie zur Vorratsdatenspeicherung 2006/24/EG³⁵ unterliegen.

29. Es gibt jedoch keine Harmonisierung auf EU-Ebene im Hinblick auf strafrechtliche Zwangsmaßnahmen und Strafverfahren zur Durchsetzung eines Rechtes des geistigen Eigentums, da auf EU-Ebene kein Einvernehmen erzielt werden konnte. Dieser Bereich fällt folglich unter die nationale Zuständigkeit, wobei ein Ausgleich der Rechte auf nationaler Ebene erzielt werden muss³⁶.
30. Die Notwendigkeit ein angemessenes Gleichgewicht zwischen dem Recht des geistigen Eigentums und den Grundrechten, wie dem Recht auf Datenschutz, zu finden, wurde vom Europäischen Gerichtshof seit dem Urteil in der Rechtssache *Promusicae*³⁷ konsequent unterstrichen und präzisiert.
31. Aus diesem Grund ist es besonders wichtig, dass die im ACTA vorgesehenen Durchsetzungsmaßnahmen dem aktuellen EU-Rechtsrahmen entsprechen, der dieses Gleichgewicht der Rechte, im Bezug auf die Durchsetzung der Rechte des geistigen Eigentums, gewährleistet.

III.4. Auswirkung von ACTA auf den zukünftigen Rechtsrahmen der EU und der Mitgliedstaaten

32. Wenn auch Artikel 27 Absatz 3 und Artikel 27 Absatz 4 des ACTA auf eine Weise formuliert sind, der zu entnehmen ist, dass die Einführung dieser Art von Maßnahmen für die Vertragsparteien nicht zwingend vorgeschrieben ist³⁸, wird darin dennoch eindeutig ausgeführt, dass die Vertragsparteien, einschließlich der EU sowie deren Mitgliedstaaten, die Möglichkeit haben, dies zu tun. Obgleich die Verwendung dieses permissiven und nicht verbindlichen Wortlauts weniger problematisch erscheinen könnte, verringert dies keineswegs die Bedenken im Hinblick auf die Einführung derartiger Mechanismen aus verschiedenen Gründen.
33. Der aus den Verhandlungen hervorgegangene Text des Übereinkommens ist nicht ausreichend präzise und lässt viel Interpretationsspielraum seitens der Vertragsparteien. Ein derartiger Mangel an Präzision ist bedauerenswert, da das Übereinkommen nicht mit ausreichender Rechtssicherheit die Arten von Mechanismen darlegt, die als Ergebnis des Beitritts zu ACTA eingerichtet werden können sowie die Sicherheiten gegen den Missbrauch personenbezogener Daten oder zum Schutz des Verteidigungsrechts.

³⁵ Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54.

³⁶ Dies ist der Grund dafür, dass der Abschnitt zur strafrechtlichen Durchsetzung im ACTA direkt von den EU-Mitgliedstaaten und nicht von der Kommission verhandelt wurde.

³⁷ Siehe insbesondere Rechtssache C-275/06 *Promusicae*, Slg. 2008, I-271, Randnummern 62 bis 68, Rechtssache C-70/10, *Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Urteil vom 24. November 2011, Randnummer 44, Rechtssache C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) gegen Netlog NV*, Urteil vom 16. Februar 2012, Randnummern 42-44, und Rechtssache C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB gegen Perfect Communication Sweden AB*, Urteil vom 19. April 2012.

³⁸ Artikel 27 Absatz 3 ist zu entnehmen, dass die Vertragsparteien „bestrebt“ sind und in Artikel 27 Absatz 4 wird das Wort „kann“ verwendet.

34. Grundsätzlich sollten die Maßnahmen, die auf EU-Ebene zur Stärkung der digitalen Rechtsdurchsetzung im Zuge des ACTA-Beitritts ergriffen werden, sich im Rahmen des EU-Rechts bewegen und die Einhaltung der von der EU gewährleisteten Grundrechte sollte sichergestellt sein. Es besteht jedoch die Gefahr, dass ACTA Auswirkungen auf den künftigen EU-Rechtsrahmen haben wird, da neue Rechtsinstrumente und Änderungen des bestehenden EU-Rechts mit der ACTA-Ratifizierung und dessen, was darin vereinbart wurde begründet werden könnten. Auch die umfassende Umsetzung von auf diesen Maßnahmen beruhenden Bestimmungen in Drittstaaten unter ACTA könnte Einfluss auf die gesetzgeberische Debatte innerhalb der EU haben. Die Kommission ist derzeit mit der Überarbeitung der Richtlinie zum geistigen Eigentum befasst und dabei könnte die Ratifizierung von ACTA einen Anreiz bieten, Durchsetzungsmechanismen einzuführen, die auf der freiwilligen Zusammenarbeit basieren, obgleich bislang kein Konsensus auf EU-Ebene erzielt wurde. Es erscheint folglich verfrüht, dass die EU sich bereits im Hinblick auf bestimmte grundlegende Prinzipien verpflichtet, insbesondere im Zusammenhang mit den Mechanismen der Zusammenarbeit zwischen Interessengruppen und Internetdiensteanbietern, wenn man berücksichtigt, dass keine Einigung bezüglich des Grundbestandteils dieser Mechanismen erzielt wurde.
35. Außerdem können die Mitgliedstaaten in der Zwischenzeit mit der Einführung eigener Maßnahmen voranschreiten. Die derzeitigen Mängel in der Formulierung des Textes sowie die Anreize, die für die Vertragsparteien geschaffen wurden, Durchsetzungsmechanismen im digitalen Umfeld in ihrem jeweils eigenen Staatsgebiet umzusetzen und auszuarbeiten, werden zersplitterten Ansätze innerhalb der EU Tür und Tor öffnen, welche wiederum das hohe Risiko einer unangemessenen oder unzureichenden Einhaltung der Datenschutzerfordernungen innerhalb der EU bergen.
36. Angesichts der obigen Ausführungen hätte der EDSB ein Übereinkommen bevorzugt, das präzisere Bedingungen und spezifische Sicherheiten enthält, was dazu beigetragen hätte, ungewollte Ansätze zu vermeiden.

IV. DETAILLIERTE ANALYSE SPEZIFISCHER BESTIMMUNGEN DES ACTA

IV.1. Der Anwendungsbereich des digitalen Kapitels und der Begriff „im gewerblichen Ausmaß“ sollten geklärt werden

37. Im digitalen Kapitel des Übereinkommens ist vorgesehen, dass die Durchsetzung primär ausgehend von den zivil- und strafrechtlichen Durchsetzungsverfahren erfolgen sollte, die in den Rechtsvorschriften der Vertragsparteien vorgesehen sind. Weitere Durchsetzungsmechanismen, die spezifisch auf das digitale Umfeld ausgerichtet sind, sind in Artikel 27 Absatz 3 und Artikel 27 Absatz 4 enthalten, obgleich nicht klar ist, inwiefern diese anderen Mechanismen in die zivil- und strafrechtlichen Mechanismen der Vertragsparteien passen würden oder ob diese Ad-hoc-Durchsetzungsmittel darstellen würden.
38. Im digitalen Kapitel wird nicht ausreichend klar definiert, welche Arten von Handlungen Gegenstand von etwaigen Durchsetzungsmaßnahmen im digitalen Umfeld wären und ob diese die Aktivitäten natürlicher Personen im Internet zu rein privaten Zwecken, wie das private Filesharing, einschließen oder ausschließen würden.
39. Diesbezüglich ist insbesondere nicht klar, ob nur diejenigen Tätigkeiten, die im „gewerblichen Ausmaß“ betrieben werden, Gegenstand der im digitalen Kapitel

enthaltenen Durchsetzungsmaßnahmen wären. Das Kriterium des „gewerblichen Ausmaßes“ wird im Übereinkommen nur im Zusammenhang mit strafrechtlichen Durchsetzungsverfahren (Artikel 23)³⁹ erwähnt, nicht aber im Hinblick auf zivilrechtliche oder andere Durchsetzungsverfahren, die im digitalen Kapitel vorgesehen sind. Dies scheint im Widerspruch zu dem EU-Ansatz der Richtlinie 2004/48/EC, in welcher der Begriff „gewerbliches Ausmaß“ auch in Bezug auf zivil- und verwaltungsrechtliche Durchsetzungsmaßnahmen verwendet wird⁴⁰, zu stehen. Folglich ist in ACTA nicht ausreichend gewährleistet, dass nur Tätigkeiten mit „gewerblichem Ausmaß“ Gegenstand der im digitalen Kapitel vorgesehenen Durchsetzungsmaßnahmen wären.

40. Außerdem führt Artikel 23 zu einer Kriminalisierung bestimmter im Internet durchgeführter Handlung, die Gegenstand von Strafen sind, „darunter Haft- und Geldstrafen, deren Höhe vor künftigen Rechtsverstößen abschreckt und die sich im Strafrahmen für Straftaten vergleichbarer Schwere bewegen“ (Artikel 24). Es wird versucht, die Kriminalisierung für bestimmte Arten von Handlungen vorzusehen, wie „vorsätzliche Copyright-Piraterie“ oder „vorsätzliche Nachahmung durch verwandte Schutzrechte geschützter Waren“ im „gewerblichen Ausmaß“, obgleich keine klare Definition dafür gegeben wird, welche Arten von Handlungen eine Straftat darstellen würden. Es gibt keinerlei Verknüpfung zwischen der Anwendung strafrechtlicher Durchsetzungsmaßnahmen und den Handlungen, die gemäß den Rechtsvorschriften der Vertragsparteien als Straftaten betrachtet werden. Artikel 23 scheint folglich neue Kategorien von Straftaten zu schaffen, die Gegenstand strafrechtlicher Durchsetzungsmaßnahmen wären, ohne dass es irgendeine Definition gäbe, die in Bezug auf strafrechtliche Sanktionen ausreichend Rechtssicherheit bieten würde.
41. Dies ist noch besorgniserregender, wenn man bedenkt, dass der Begriff im „gewerblichen Ausmaß“ selbst nicht so genau definiert wird, dass Rechtssicherheit bestünde im Hinblick auf den Anwendungsbereich der Durchsetzungsmaßnahmen in der digitalen Umgebung in Zusammenhang mit Handlungen, die von natürlichen Personen zum privaten Gebrauch durchgeführt werden. Artikel 23 führt in Zusammenhang mit strafrechtlichen Durchsetzungsmaßnahmen Folgendes aus: „in gewerblichem Ausmaß vorgenommene Rechtsverletzungen zeichnen sich dadurch aus, dass sie zwecks Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteils vorgenommen werden“. Der Begriff des „mittelbaren“ wirtschaftlichen oder kommerziellen Vorteils ist jedoch sehr weit gefasst und kann sehr weit ausgelegt werden und somit eine Reihe von Tätigkeiten umfassen, die von natürlichen Personen im Internet zu rein privaten Zwecken durchgeführt werden und aus denen diese keinen wirtschaftlichen Gewinn oder Vorteil ziehen. Außerdem enthält Artikel 23 keine erschöpfende Liste der Handlungen, welche unter den Begriff im gewerblichen Ausmaß fallen würden (Verwendung des Begriffs „zumindest“). Dies kann im Widerspruch zur Auslegung des Begriffs in „gewerblichen Ausmaß“ in der EU stehen, wo davon ausgegangen wird, dass „(...) in der Regel Handlungen [ausgeschlossen sind], die in gutem Glauben von Endverbrauchern vorgenommen werden“⁴¹ und dass „Handlungen privater Nutzer für persönliche und nicht gewinnorientierte Zwecke hierin nicht

³⁹ Artikel 23 sieht Folgendes vor „Jede Vertragspartei sieht Strafverfahren und Strafen vor, die zumindest bei vorsätzlicher Nachahmung von Markenwaren oder vorsätzlicher unerlaubter Herstellung urheberrechtlich oder durch verwandte Schutzrechte geschützter Waren in gewerblichem Ausmaß Anwendung finden“.

⁴⁰ Der Erwägungsgrund 14 besagt Folgendes: „Nur bei in gewerblichem Ausmaß vorgenommenen Rechtsverletzungen müssen die Maßnahmen nach Artikel 6 Absatz 2, Artikel 8 Absatz 1 und Artikel 9 Absatz 2 angewandt werden. Unbeschadet davon können die Mitgliedstaaten diese Maßnahmen auch bei anderen Rechtsverletzungen anwenden (...)“.

⁴¹ Siehe Erwägungsgrund 14 der Richtlinie 2004/48/EG.

enthalten“ sind⁴².

42. In der Folge unterstreicht der EDSB, dass das Übereinkommen im Hinblick auf den Anwendungsbereich der Durchsetzungsmaßnahmen im digitalen Umfeld nicht klar ist und dass unklar ist, ob diese ausschließlich auf großangelegte Verletzungen der Rechte des geistigen Eigentums ausgerichtet sind. Er bedauert, dass der Begriff „gewerbliches Ausmaß“ nicht ausreichend genau definiert ist und dass Handlungen, die von privaten Nutzern zu persönlichen Zwecken ohne Gewinnabsicht durchgeführt werden, nicht ausdrücklich von dem Anwendungsbereich des Übereinkommens ausgenommen sind.

IV.2. Der Anordnungsmechanismus und die Überwachung von Internet-Nutzern durch Rechteinhaber

43. Zur Stärkung der Durchsetzung von Rechten des geistigen Eigentums im digitalen Umfeld sieht Artikel 27 Absatz 4 des Übereinkommens die Möglichkeit vor, dass die Vertragsparteien einen spezifischen Anordnungsmechanismus einrichten, der an die Internetdiensteanbieter gerichtet ist⁴³. Dieses Anordnungsverfahren würde es den „zuständigen Behörden“ erlauben, Internetdiensteanbietern gegenüber anzuordnen, einem Rechteinhaber „unverzüglich“ die nötigen Informationen zur Identifizierung eines solchen Abonnenten offenzulegen, dessen Konto zur mutmaßlichen Rechtsverletzung genutzt wurde.
44. Der Einsatz eines solchen Anordnungsmechanismus setzt voraus, dass der Rechteinhaber eine Form der Überwachung der Internetnutzung durchführt, um Konten zu identifizieren, die „zur mutmaßlichen Rechtsverletzung genutzt werden“. Dies bedeutet die Verarbeitung sensibler Daten im Zusammenhang mit mutmaßlichen Straftaten oder strafrechtlichen Verurteilungen, die gemäß Artikel 8 Absatz 5 der Richtlinie 95/46/EG „nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen“ darf. Während die Verarbeitung von Daten durch Rechteinhaber im Zusammenhang mit dem Verdacht auf Verletzung von Rechten des geistigen Eigentums unter spezifischen Bedingungen zu Zwecken eines eigenen Rechtsstreits zulässig sein kann, sollte sie dennoch nicht über das hinausgehen, was zu diesem Zweck notwendig und verhältnismäßig ist.
45. In diesem Zusammenhang dürften – wie in Abschnitt III.2 oben erläutert – aus der Sicht des Datenschutzes Rechteinhaber nur dann an zielgerichteten Überwachungen im

⁴² Legislative Entschließung des Europäischen Parlaments vom 25. April 2007 zu dem geänderten Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Maßnahmen zur Durchsetzung der Rechte des geistigen Eigentums (KOM(2006) 0168 - C6-0233/2005 - 2005/0127(CODI)), *ABl. C 74E vom 20.3.2008*, S. 526. Siehe auch Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Maßnahmen zur Durchsetzung der Rechte des geistigen Eigentums“, KOM(2005) 276 endg. — 2005/0127 (COD), *Abl. C 256 vom 27.10.2007*, S. 0003-0007. Insbesondere, dass „Davon abgesehen sind der private Austausch von Internetdateien, die Vervielfältigung (bzw. der Remix von Musiktiteln) oder die Wiedergabe materieller oder geistiger Werke im familiären oder privaten Rahmen oder zu Studien- und Versuchszwecken stillschweigend aus dem Anwendungsbereich der vorgeschlagenen Rechtsetzung ausgeschlossen; dieser Ausschluss sollte ausdrücklich erfolgen“.

⁴³ Gemäß Artikel 27 Absatz 4 kann eine Vertragspartei „in Übereinstimmung mit ihren Rechts- und Verwaltungsvorschriften ihre zuständigen Behörden dazu ermächtigen, einem Onlinediensteanbieter gegenüber anzuordnen, einem Rechteinhaber unverzüglich die nötigen Informationen zur Identifizierung eines Abonnenten offenzulegen, dessen Konto zur mutmaßlichen Rechtsverletzung genutzt wurde, falls dieser Rechteinhaber die Verletzung eines Marken-, Urheber- oder verwandten Schutzrechts rechtsgenügend geltend gemacht hat und die Informationen zu dem Zweck eingeholt werden, diese Rechte zu schützen oder durchzusetzen.“

Kontext beschränkter, spezifischer Ad-hoc-Situationen beteiligt sein, in denen ein begründeter Verdacht einer Verletzung des Urheberrechts im gewerblichen Ausmaß besteht.⁴⁴ Außerdem sollte angesichts der spezifischen Gefahren für die Rechte und Freiheiten natürlicher Personen die zielgerichtete Überwachung zusätzlichen datenschutzrechtlichen Sicherheiten unterliegen, wie der Vorabkontrolle oder der Genehmigung durch die jeweiligen nationalen Datenschutzbehörden⁴⁵.

46. Aus verfahrenstechnischer Sicht sollte die Verarbeitung von Strafverfolgungsdaten durch private Parteien, insbesondere die Offenlegung personenbezogener Daten, welche die Identifizierung von verdächtigen Abonnenten zu Zwecken der Durchsetzung von Rechten des geistigen Eigentums erlauben, durch Internetdiensteanbieter an Rechteinhaber unter der Kontrolle einer Justizbehörde erfolgen.⁴⁶ Dies ist gegenwärtig der Fall im Hinblick auf die Offenlegung personenbezogener Daten im Kontext zivilrechtlicher Verfahren im Rahmen der Richtlinie zum geistigen Eigentum, deren Artikel 8 vorsieht, dass 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) offenlegen. Die Beteiligung von Justizbehörden ist ein wesentlicher Teil des aktuellen EU-Systems und von wesentlicher Bedeutung, um sicherzustellen, dass die Durchsetzung unter Einhaltung des Grundsatzes eines fairen Verfahrens und der Grundrechte stattfindet.
47. Es ist jedoch nicht klar, wer die „zuständigen Behörden“ sind, die mit einer solchen Anordnungsbefugnis gemäß Artikel 27 Absatz 4 des Übereinkommens ausgestattet wären. Die Verwendung des vagen Begriffs „zuständige Behörden“ bietet nicht viel Rechtssicherheit dafür, dass die Offenlegung personenbezogener Daten im Rahmen dieser Bestimmung lediglich unter der Kontrolle von Justizbehörden stattfinden würde. Ganz im Gegenteil: Dieser Begriff könne auch Verwaltungsbehörden umfassen, die mit spezifischen justizähnlichen Aufgaben betraut wurden, ohne jedoch die Garantien, im Hinblick auf die Unabhängigkeit, Unparteilichkeit und Einhaltung der Rechte auf Unschuldsvermutung und auf einen fairen Prozess, erbringen zu können, die für Justizorgane gelten.
48. Außerdem sind auch die von den Rechteinhabern einzuhaltenden Bedingungen dafür, eine solche Anordnung zu erhalten, nicht besonders zufriedenstellend. Der Rechteinhaber muss „die Verletzung eines Marken-, Urheber- oder verwandten Schutzrechts rechtsgenügend geltend gemacht“ haben und muss die Informationen zu dem Zweck eingeholt haben, „diese Rechte zu schützen oder durchzusetzen“. Diese

⁴⁴ Vgl. Absätze 45 ff. der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

⁴⁵ Artikel 20 der Richtlinie 95/46/EG gestattet es den Mitgliedstaaten festzulegen, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

⁴⁶ Stellungnahme der Datenschutzgruppe „Artikel 29, WP104, Seite 7: Gemäß Artikel 8 Absatz 5 der Datenschutzrichtlinie darf die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, nur unter strengen, von den Mitgliedstaaten festgelegten Voraussetzungen erfolgen. 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.“

Formulierung ist wesentlich schwächer als diejenige der Richtlinie zum geistigen Eigentum, wonach eine Anordnung auf einen „*begründeten und die Verhältnismäßigkeit wahren Antrag*“ hin nur unter der Bedingung gewährt werden würde, dass der Antrag „im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums“ gestellt wird. Gemäß der Richtlinie zum geistigen Eigentum ist es Sache der Gerichte, die Fakten und die Schwere des angeblichen Fehlverhaltens von Fall zu Fall zu bewerten sowie dessen Umfang und Gefahren für das Recht auf Privatsphäre, um zu entscheiden ob diese Informationen offengelegt werden oder nicht.

49. Die Ungewissheiten in Artikel 27 Absatz 4 können bei extraterritorialen Anordnungen zuständiger ausländischer Behörden an Internetdiensteanbieter mit Sitz in Europa wesentliche Auswirkungen haben. Der aktuelle Wortlaut des Übereinkommens kann Anordnungen an Internetdiensteanbieter mit Sitz in der EU von ausländischen Organen, die keine Justizorgane sind, zur Offenlegung von Informationen, welche es den Rechteinhabern erlauben, deren in der EU ansässigen Internet-Abonnenten zu identifizieren, legitimieren, selbst wenn diese Anordnungen außerhalb des Rahmens eines laufenden Gerichtsverfahrens ausgesprochen werden. Dies bedeutet, dass der Schutz der Rechte natürlicher Personen, den die in der EU ansässigen Internet-Abonnenten gemäß EU-Recht genießen, in einem derartigen Kontext nicht mehr in angemessener Weise sichergestellt wäre.

IV.3. Mechanismen zur Zusammenarbeit bei der Durchsetzung und Überwachung des Internets seitens der Internetdiensteanbieter

50. Wie in Abschnitt III.1 oben erläutert, zielt Artikel 27 Absatz 3 auf die freiwillige Einführung „privater“ Durchsetzungsmechanismen ab, die auf der freiwilligen Zusammenarbeit zwischen Rechteinhabern und Internetdiensteanbietern basieren.
51. Das Ausmaß und die Form der Zusammenarbeit kann variieren: (i) im Kontext der Three-Strikes-Regelungen werden die Internetdiensteanbieter in der Regel dazu aufgefordert, ihre Abonnenten zu identifizieren, um diese zu warnen, was zur Vertragsbeendigung führen könnte; (ii) die Internetdiensteanbieter werden auch von den Rechteinhabern aufgefordert, in deren Namen die Überwachung verdächtiger Verhaltensweisen im Internet durchzuführen, wie bei den Three-Strikes-Regelungen oder zur Überwachung von Webseiten, die mutmaßlich strafwürdige Inhalte enthalten und (iii) sie können außerdem von Rechteinhabern aufgefordert werden, technische Instrumente umzusetzen, um den Peer-to-Peer-Datenverkehr zu filtern und mutmaßlich strafwürdige Inhalte zu sperren, was zu einer Überwachung von natürlichen Personen und deren elektronischer Kommunikation auf großer Skala führen kann.
52. Diese Formen von Mechanismen der Zusammenarbeit zur Rechtsdurchsetzung, welche die Verarbeitung personenbezogener Daten durch die Internetdiensteanbieter zu Zwecken der Durchsetzung von Rechten des geistigen Eigentums und/oder die Überwachung der Verhaltensweisen natürlicher Personen, einschließlich der elektronischen Kommunikation auf großer Skala, mit sich bringen, werfen aus der Sicht des Schutzes der Privatsphäre und des Datenschutzes ernsthafte Bedenken auf. Sie können außerdem zur Sperrung des Internet-Zugangs oder von Webseiten führen, was einen Eingriff in Grundfreiheiten darstellen kann, wie die Freiheit der

Meinungsäußerung und die Freiheit, Informationen zu erhalten oder weiterzugeben und des Zugangs zu Kultur⁴⁷.

53. Es muss sichergestellt werden, dass die Rolle, welche die Internetdiensteanbieter im Rahmen der Mechanismen der Zusammenarbeit zur Durchsetzung von Rechten einnehmen sollen, die entweder durch neue Rechtsinstrumente eingeführt werden oder auf Antrag der Rechteinhaber im Rahmen privater Vereinbarungen stattfinden, vereinbar ist mit deren aus EU-Recht erwachsenden Rechten und Pflichten sowie mit dem Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen in der EU. Die jüngste Rechtsprechung des Gerichtshofs in Bezug auf Maßnahmen, die Internetdiensteanbietern zu Zwecken der Durchsetzung von Rechten des geistigen Eigentums auferlegt werden, ist besonders erhellend, da darin die Grenzen dessen geklärt werden, was Internetdiensteanbieter im Rahmen der Durchsetzung von Rechten des geistigen Eigentums im Internet gemäß EU-Recht dürfen.
54. Erstens kann Internetdiensteanbietern gemäß dem aktuellen Haftungssystem der Internetdiensteanbieter, das in der Richtlinie über den elektronischen Geschäftsverkehr, insbesondere in Artikel 15 Absatz 1⁴⁸ enthalten ist, keine Maßnahme auferlegt werden, welche die Durchführung einer generellen Überwachung der über deren Netz laufenden Informationen erforderlich macht. In *Scarlet gegen Sabam*⁴⁹ analysierte der Gerichtshof die Verarbeitung von Daten seitens eines Internetdiensteanbieters, der aufgefordert worden war, eine Maßnahme zur Filterung von Daten umzusetzen, um Verletzungen der Rechte des geistigen Eigentums vorzubeugen. Der Gerichtshof stellte fest, dass eine solche Filterungsmaßnahme dazu führen würde, dass ein Internetdiensteanbieter aktiv alle Daten im Zusammenhang mit den eigenen Kunden und die gesamte über dieses Netz laufende elektronische Kommunikation überwachen müsste, ganz gleich, ob es dabei zu illegalen Downloadaktivitäten kommt oder nicht. Der Gerichtshof kam zu der Schlussfolgerung, dass eine solche Filterungsmaßnahme zu einer allgemeinen Überwachungspflicht führen würde, die nicht mit Artikel 15 Absatz 1 der Richtlinie über den elektronischen Geschäftsverkehr 2000/31/EG vereinbar ist.
55. Zweitens gehen diese Arten von Maßnahmen über den Rahmen der Verarbeitung hinaus, welche Internetdiensteanbieter rechtmäßig gemäß den Datenschutzbestimmungen und insbesondere gemäß der Datenschutzrichtlinie für elektronische Kommunikation durchführen dürfen. Es gibt weder in der Datenschutzrichtlinie für elektronische Kommunikation noch in der Richtlinie zur Datenvorratsspeicherung 2006/24/EG eine Rechtsgrundlage dafür, dass Internetdiensteanbieter die Verbindungen zwischen den einzelnen IP-Adressen und der Internetnutzung zum Zwecke der längerfristigen Überwachung oder Analyse mit dem Ziel der Identifizierung „möglicher“ Verletzer von Rechten des geistigen Eigentums aufbewahren⁵⁰. Außerdem bedeutet die Tatsache, dass Internetdiensteanbieter über bestimmte Daten verfügen, nicht, dass diese Daten zu einem anderen Zweck an die Urheberrechteinhaber übermitteln können. Diesbezüglich beschränkt sich die Offenlegung von Informationen gemäß der Richtlinie zur Vorratsdatenspeicherung auf eine Übermittlung an die zuständigen nationalen Behörden

⁴⁷ Diese Aspekte seien an dieser Stelle lediglich angeführt, sie werden jedoch nicht weiter erörtert, da in dieser Stellungnahme nur Fragen im Zusammenhang mit dem Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen behandelt werden.

⁴⁸ Artikel 15 Absatz 1 der Richtlinie 2000/31/EG sieht Folgendes vor: „Die Mitgliedstaaten erlegen Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen“.

⁴⁹ Siehe Fußnote 37.

⁵⁰ Siehe Absätze 54 bis 60 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

„zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden“⁵¹. Außerdem würde die Überwachung der über deren Netze laufenden elektronischen Kommunikation die Vertraulichkeit der Kommunikation gemäß Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation verletzen, ohne dass dies unter eine der in Artikel 15 der genannten Richtlinie vorgesehenen Ausnahmen fallen würde. Abschließend würde die Offenlegung von Daten bezüglich der elektronischen Kommunikation durch Internet-Diensteanbieter an Dritte ohne die Zustimmung der Nutzer Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation verletzen.

56. Drittens, wie in Abschnitt III.2 oben erklärt, können diese Arten von Maßnahmen zu einer Überwachung der Aktivitäten von Internetnutzern führen, die zur Erreichung des Ziels der Durchsetzung von Rechten des geistigen Eigentums unverhältnismäßig ist. Diesbezüglich führte der Gerichtshof im Urteil in der Rechtssache *Scarlet gegen Sabam*⁵² an, dass eine Maßnahme, welche die Überwachung der gesamten elektronischen Kommunikation umfasst, die im Hinblick auf den Anwendungsbereich, den Zeitraum und die betreffenden Personen nicht gut definiert und genau ist, nicht die Vorgabe bezüglich eines angemessenen Gleichgewichts zwischen Rechten des geistigen Eigentums und anderen Grundrechten und Freiheiten erfüllen würde⁵³.
57. Abschließend sollten freiwillige Mechanismen der Zusammenarbeit zur Durchsetzung nicht als ein Mittel eingesetzt werden, um das Gesetz zu umgehen. Der EDSB ist der Ansicht, dass nicht ausreichend sichergestellt ist, dass freiwillige Maßnahmen, die von privaten Akteuren ausgehend von ACTA ergriffen werden, nicht über das angemessene Gleichgewicht zwischen den Rechten des geistigen Eigentums und des Datenschutzes hinausgehen würden.

IV.4. Zusammenarbeit und grenzüberschreitender Datenaustausch

58. Mehrere ACTA-Bestimmungen sehen den internationalen Datenaustausch vor, wie beispielsweise zwischen Grenzbehörden (Artikel 29) und zwischen öffentlichen Behörden (Artikel 34). Die ACTA-Bestimmungen zum Informationsaustausch und zur Zusammenarbeit sind so allgemein formuliert, dass es besonders unklar ist, welche Art von Daten ausgetauscht werden können und zwischen wem. Dieser Austausch könnte sich auf jede Art der Information beziehen, einschließlich personenbezogener Daten im Zusammenhang mit dem Verdacht von Verletzungen der Rechte des geistigen Eigentums. Außerdem können andere ACTA-Bestimmungen den internationalen Informationsaustausch zwischen privaten Parteien und/oder zwischen öffentlichen und privaten Parteien zur Folge haben (z. B. im Kontext der in Artikel 11 und Artikel 27 Absatz 4 vorgesehenen Durchsetzungsverfahren).
59. Erstens unterstreicht der EDSB, dass bei allen Verfahren, die im Übereinkommen vorgesehen sind, welche zur Verarbeitung personenbezogener Daten natürlicher Personen im Anwendungsbereich des EU-Rechts führen, die Datenschutzbestimmungen einzuhalten sind; dieser Schutz umfasst alle Kategorien natürlicher Personen, ungeachtet

⁵¹ Siehe Artikel 4 der Richtlinie zur Vorratsdatenspeicherung sowie Rechtssache C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB gegen Perfect Communication Sweden AB*, Urteil vom 19. April 2012, Randnummer 41.

⁵² Siehe Fußnote 37.

⁵³ Siehe Randnummer 45 ff. des Urteils.

deren Nationalität oder Ansässigkeit, einschließlich denjenigen, die verdächtigt werden oder potenziell an groß angelegter Produktfälschung und -piraterie beteiligt sind.

60. Wie bei allen Maßnahmen, die Auswirkungen auf die Rechte auf den Schutz der Privatsphäre und den Datenschutz natürlicher Personen haben, müssen die Übermittlungen personenbezogener Daten in diesem Kontext der Prüfung auf Einhaltung des Prinzips der Notwendigkeit und Verhältnismäßigkeit standhalten. Der EDSB hat bereits in seiner früheren Stellungnahme unterstrichen, dass die Prinzipien der Notwendigkeit und der Verhältnismäßigkeit der Datenübermittlungen einfacher einzuhalten wären, 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 gestatten⁵⁴. Dies wurde jedoch nicht beachtet, da die Formulierung des Abkommens im Hinblick auf den Anwendungsbereich der Durchsetzungsverfahren besonders unklar ist (wie in Abschnitt IV.1 oben erläutert).
61. Außerdem muss die Übermittlung personenbezogener Daten an Empfänger außerhalb der EU im Einklang mit den Datenschutzerfordernungen erfolgen. In Artikel 25 und 26 der Richtlinie 95/46/EG sind die Bedingungen enthalten, unter denen eine internationale Übermittlung personenbezogener Daten durchgeführt werden kann. Es gelten spezifische Regeln im Hinblick auf die Datenübermittlungen im Bereich der Strafverfolgung, die im Übereinkommen des Europarats Nr. 108 und dem Zusatzprotokoll⁵⁵ und im Rahmenbeschluss 2002/584/JI des Rates⁵⁶ enthalten sind. All diese Bestimmungen basieren auf gemeinsamen Grundsätzen, insbesondere auf dem Grundsatz, dass Übermittlungen an Empfänger in Staaten, die kein angemessenes Schutzniveau bieten, Gegenstand zusätzlicher Garantien sein müssen, die eindeutig in rechtlich verbindlichen Instrumenten festgelegt werden (wie die Menge und die Arten der übermittelten Daten, Einschränkungen im Hinblick auf die weitere Übermittlung, Fristen für die Datenaufbewahrung, Überwachung und effektive Rückgriffsmechanismen).
62. Als Ergebnis unterstreicht der EDSB, dass die EU spezifische Vereinbarungen mit ihren Handelspartnern abschließen sollte, um angemessene Datenschutzgarantien für den Austausch personenbezogener Daten mit Empfängern in diesen Staaten sicherzustellen.

IV.5. Der Mangel an angemessenen Garantien in ACTA

63. Gemäß Artikel 27 Absatz 2, Artikel 27 Absatz 3 und Artikel 27 Absatz 4 müssen die im digitalen Umfeld umgesetzten Durchsetzungsmaßnahmen die „Grundsätze wie freie Meinungsäußerung, faires Gerichtsverfahren und Schutz der Privatsphäre“ wahren. Der EDSB unterstreicht, dass allein der Verweis auf diese Grundsätze nicht ausreichend ist. Daneben ist nicht klar, auf was sich die „wesentlichen Grundsätze“ und „das faire Gerichtsverfahren“ beziehen.

⁵⁴ Siehe Randnummer 67 der Stellungnahme des EDSB vom 22. Februar 2010 zu ACTA.

⁵⁵ Europäisches Übereinkommen Nr. 108 zum 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.

⁵⁶ 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.

64. Auf internationaler Ebene werden die Meinungsfreiheit und der Schutz der Privatsphäre in der Universellen Erklärung der Menschenrechte als Grundrechte und nicht einfach als „Grundsätze“ anerkannt. Außerdem entspricht der Begriff des „fairen Gerichtsverfahrens“ keinem allgemein anerkannten Menschenrecht. Es scheint hier eine Mischung aus zwei verschiedenen rechtlichen Konzepten vorzuliegen, auf der einen Seite das Recht auf einen fairen Prozess (das in Artikel 10 der Universellen Erklärung der Menschenrechte und in Artikel 47 der Charta der Grundrechte der Europäischen Union verankert ist) und auf der anderen Seite der Begriff des „fairen Verfahrens“ (das beispielsweise in der Verfassung der Vereinigten Staaten als ein Mittel zum Schutz einer Person vor der Beraubung des Lebens, der Freiheit oder des Eigentums ohne ein gerechtes Verfahren vorgesehen ist).
65. Es sei unterstrichen, dass die Europäische Union im Kontext der Revision der oben genannten Richtlinie 2002/21/EG die Garantien präzise dargelegt hat, die erforderlich sind für die Umsetzung von Maßnahmen, die den Zugang und die Nutzung von Dienstleistungen und Anwendungen über elektronische Kommunikationsnetze seitens der Endnutzer betreffen. Sie umfassen insbesondere angemessene Verfahrensgarantien in Übereinstimmung mit der Europäischen Menschenrechtskonvention und den allgemeinen Grundsätzen des Gemeinschaftsrechts, einschließlich der Grundsätze des effektiven gerichtlichen Schutzes, des ordnungsgemäßen Verfahrens, der Unschuldsannahme und des Rechts auf Privatsphäre⁵⁷.
66. Der EDSB unterstreicht die Vorteile eines Ansatzes, der die Einschränkungen und Garantien eindeutig bestimmt, innerhalb welcher Maßnahmen, welche die Nutzung und die Überwachung der elektronischen Kommunikationsnetze berühren, stattfinden können. Es wäre folglich besser gewesen, wenn ACTA diese Garantien klar festgelegt hätte.

V. SCHLUSSFOLGERUNG

67. Obgleich der EDSB das berechtigte Interesse daran anerkennt, die Durchsetzung von Rechten des geistigen Eigentums in einem internationalen Kontext sicherzustellen, muss ein Mittelweg gefunden werden zwischen den Forderungen nach Schutz von Rechten

⁵⁷ Artikel 1 Absatz 1 Buchstabe b der Richtlinie 2009/140/EG, der einen neuen Absatz (Absatz 3 Buchstabe a) in Artikel 1 der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (die so genannte „Änderung 138“) einführt: „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.“

des geistigen Eigentums und dem Recht natürlicher Personen auf Schutz der Privatsphäre und auf Datenschutz.

68. Der EDSB unterstreicht, dass die angestrebten Mittel zur Stärkung der Durchsetzung der Rechte des geistigen Eigentums nicht auf Kosten der Grundrechte und Freiheiten natürlicher Personen auf den Schutz der Privatsphäre, des Datenschutzes und der Freiheit zur Meinungsäußerung sowie anderer Rechte wie der Unschuldsannahme und des effektiven gerichtlichen Schutzes gehen dürfen.
69. Viele der im Übereinkommen angestrebten Maßnahmen im Kontext der Durchsetzung von Rechten des geistigen Eigentums im digitalen Umfeld hätten die Überwachung der Verhaltensweisen der Nutzer und derer elektronischen Kommunikation im Internet zur Folge. Diese Maßnahmen stellen einen wesentlichen Eingriff in die Privatsphäre natürlicher Personen dar und können, sofern sie nicht ordnungsgemäß umgesetzt werden, einen Eingriff in deren Rechte und Freiheiten darstellen, unter anderem in das Recht auf Schutz der Privatsphäre, Datenschutz und Geheimhaltung der Kommunikation.
70. Es sollte sichergestellt werden, dass alle etwaigen Online-Durchsetzungsmaßnahmen, die innerhalb der EU aufgrund des Beitritts zu ACTA umgesetzt werden, notwendig sind und in einem angemessenen Verhältnis zu den rechtmäßig verfolgten Zielen stehen. Der EDSB unterstreicht, dass Maßnahmen, welche die wahllose oder ausgedehnte Überwachung der Verhaltensweisen von Internetnutzern im Zusammenhang mit unbedeutenden Rechtsverletzungen auf kleiner Skala, mit denen keine Gewinnabsicht verbunden ist, zur Folge hätten, unangemessen und nicht mit Artikel 8 EMRK, den Artikeln 7 und 8 der Charta der Grundrechte und der Datenschutzrichtlinie vereinbar wären.
71. Der EDSB hat außerdem spezifische Bedenken im Zusammenhang mit verschiedenen Bestimmungen des Übereinkommens:
 - Im Übereinkommen ist der Anwendungsbereich der Durchsetzungsmaßnahmen im digitalen Umfeld, die in Artikel 27 vorgesehen sind, nicht klar definiert und es ist nicht klar, ob diese sich nur auf groß angelegte Verletzungen der Rechte des geistigen Eigentums beziehen. Der Begriff „gewerbliches Ausmaß“ in Artikel 23 des Übereinkommens ist nicht ausreichend genau definiert und Handlungen, die von privaten Nutzern zu persönlichen Zwecken ohne Gewinnabsicht durchgeführt werden, sind nicht ausdrücklich von dem Anwendungsbereich des Übereinkommens ausgenommen.
 - Der Begriff „zuständige Behörden“, die gemäß Artikel 27 Absatz 4 mit einer Anordnungsbefugnis ausgestattet werden, ist zu vage und stellt nicht ausreichend sicher, dass die Offenlegung personenbezogener Daten mutmaßlicher Rechtsverletzer nur unter der Aufsicht der Justizbehörden erfolgt. Außerdem sind auch die von den Rechteinhabern einzuhaltenden Bedingungen dafür, eine solche Anordnung zu erhalten, nicht zufriedenstellend. Diese Unsicherheiten können insbesondere bei Anfragen ausländischer zuständiger Behörden an Internetdiensteanbieter in der EU von Bedeutung sein.

- Viele der freiwilligen Maßnahmen der Zusammenarbeit zur Rechtsdurchsetzung, die auf der Grundlage von Artikel 27 Absatz 3 des Übereinkommens umgesetzt werden könnten, würden zu einer Verarbeitung personenbezogener Daten durch die Internetdiensteanbieter führen, die über das hinausgeht, was gemäß EU-Recht vorgesehen ist;
- Die Vereinbarung enthält keine ausreichenden Einschränkungen und Garantien bezüglich der Umsetzung von Maßnahmen, welche zur groß angelegten Überwachung elektronischer Kommunikationsnetzwerke führen würden. Insbesondere sind keine Garantien, wie die Einhaltung der Rechte auf Schutz der Privatsphäre und Datenschutz, auf einen effektiven gerichtlichen Schutz, ein ordnungsgemäßes Verfahren und die Unschuldsannahme enthalten.

Brüssel, den 24. April 2012

(unterzeichnet)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter