I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten

(2012/C 34/01)

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 7 und 8,

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

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 Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ([2]), insbesondere auf Artikel 41 Absatz 2,

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 ([3]) —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

I.1 Hintergrund

1. Am 19. April 2011 nahm die Kommission eine Mitteilung „Offenes Internet und Netzneutralität in Europa“ an ([4]).

2. Die vorliegende Stellungnahme kann als Reaktion des EDSB auf diese Mitteilung aufgefasst werden; sie möchte einen Beitrag zur derzeit laufenden Debatte in der EU über Netzneutralität, insbesondere über die Aspekte Datenschutz und Schutz der Privatsphäre leisten.

([1]) ABl. L 281 vom 23.11.1995, S. 31 („Datenschutzrichtlinie“).
([2]) ABl. L 8 vom 12.1.2001, S. 1 („Datenschutzverordnung“).
([3]) ABl. L 201 vom 31.7.2002, S. 37, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (siehe Fußnote 15) („Datenschutzrichtlinie für elektronische Kommunikation“).
([4]) KOM(2011) 222 endg.

3. Die Stellungnahme stützt sich auf die Antwort ([5]) des EDSB in der von der Kommission im Vorfeld der Mitteilung abgehaltenen öffentlichen Konsultation zum Thema „Offenes Internet und Netzneutralität in Europa". Des Weiteren hat der EDSB den kürzlich formulierten Entwurf von Schlussfolgerungen des Rates zum Thema Netzneutralität berücksichtigt ([6]).

I.2 **Das Konzept der Netzneutralität**

4. Die Netzneutralität ist Gegenstand einer derzeit stattfindenden Debatte über die Frage, ob es Internetdienstanbietern ([7]) gestattet sein sollte, den Zugang zum Internet zu begrenzen, zu filtern oder zu sperren oder seine Leistungsfähigkeit anderweitig zu beeinflussen. Das Konzept der Netzneutralität stützt sich auf die Ansicht, dass Daten über das Internet unparteiisch übermittelt werden sollten, unabhängig von Inhalt, Ziel oder Quelle, und dass die Nutzer darüber entscheiden können sollten, welche Anwendungen, Dienste und Hardware sie verwenden möchten. Das bedeutet, dass Internetdiensteanbieter nicht willkürlich den Zugang zu bestimmten Anwendungen oder Diensten wie Peer-to-Peer („P2P") usw. vorrangig behandeln oder verlangsamen können ([8]).

5. Das Filtern, Sperren und Untersuchen des Datenverkehrs wirft häufig übersehene oder an den Rand gedrängte erhebliche Fragen im Zusammenhang mit der Vertraulichkeit der Kommunikation und der Wahrung der Privatsphäre von Personen und des Schutzes ihrer personenbezogenen Daten bei der Nutzung des Internets auf. Bei bestimmten Untersuchungstechniken werden beispielsweise der Inhalt des Datenverkehrs, die besuchten Websites, die gesendeten und empfangenen E-Mails, die Uhrzeiten der einzelnen Vorgänge usw. überwacht; damit ist ein Filtern des Datenverkehrs möglich.

6. Mit der Kontrolle von Kommunikationsdaten können Internetdienstanbieter die Vertraulichkeit der Kommunikation verletzen, ein Grundrecht, das in Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten („EMRK") sowie in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union („Charta") verankert ist. Die Vertraulichkeit wird ferner im Sekundärrecht der EU geschützt, insbesondere in Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation.

I.3 **Schwerpunkt und Struktur der Stellungnahme**

7. Nach Auffassung des EDSB muss sich eine ernsthafte politische Debatte über Netzneutralität mit der Vertraulichkeit des Datenverkehrs sowie anderen Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz befassen.

8. Die vorliegende Stellungnahme möchte einen Beitrag zu dieser Debatte in der EU leisten. Sie hat sich drei Ziele gesetzt:

   — Sie unterstreicht die Relevanz des Schutzes des Privatsphäre und des Datenschutzes in der derzeitigen Debatte über Netzneutralität. So geht sie insbesondere auf die Notwendigkeit ein, bestehende Vorschriften über die Vertraulichkeit des Datenverkehrs einzuhalten. Es sollten nur Vorgehensweisen zugelassen werden, die diesen Vorschriften entsprechen.

   — Netzneutralität ist im Zusammenhang mit relativ neuen — technologischen — Möglichkeiten zu sehen; daher liegen nur geringe Erfahrungen mit der Anwendung des Rechtsrahmens vor. Die Stellungnahme gibt daher Hinweise dazu, wie Internetdienstanbieter den datenschutzrechtlichen Rahmen anzuwenden haben, wenn sie ein Filtern, Sperren und Untersuchen des Datenverkehrs planen. Dies ist als Hilfestellung für die Internetdiensteanbieter, aber auch für die Behörden gedacht, die mit der Durchsetzung des Rahmens beauftragt sind.

   — Im Anwendungsbereich des Datenschutzes und des Schutzes der Privatsphäre identifiziert die Stellungnahme bestimmte Gebiete, die besondere Aufmerksamkeit verdienen und unter Umständen ein Tätigwerden auf EU-Ebene erfordern. Dies ist besonders wichtig im Hinblick auf die derzeitige Debatte auf EU-Ebene sowie auf die politischen Maßnahmen, die die Kommission in diesem Zusammenhang eventuell plant.

([5]) Der EDSB unterstrich in seiner Antwort die Bedeutung der Berücksichtigung von Fragen des Datenschutzes und des Schutzes der Privatsphäre in Verbindung mit anderen Rechten und Werten. Die Antwort kann unter folgender Adresse abgerufen werden: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Abrufbar unter http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Dazu gehört auch die Bereitstellung des Internetzugangs über das Fest- und das Mobilfunknetz.

([8]) Der Grundsatz gilt nicht für Internetdienstanbieter, die die Geschwindigkeit, mit der Daten übertragen werden, oder die Datenmenge, die ein Nutzer senden und empfangen kann, begrenzen, etwa über Zugangsverträge mit Geschwindigkeits- oder Volumengrenzen. Nach einem Grundsatz der Netzneutralität könnten Internetdienstanbieter daher weiterhin Internet-Abonnements anbieten, bei denen der Zugang nach Kriterien wie Geschwindigkeit oder Datenmenge begrenzt wird, solange dies keine Diskriminierung zum Vor- oder Nachteil bestimmter Inhalte erfordert.

9. Der EDSB ist sich der Tatsache bewusst, dass die Netzneutralität noch andere Fragen aufwirft, auf die weiter unten näher eingegangen wird; dazu gehören auch Fragen des Zugangs zu Informationen. Diese Fragen werden jedoch nur insoweit aufgegriffen, als sie mit Datenschutz und Schutz der Privatsphäre zu tun haben oder sich darauf auswirken.

10. Die Stellungnahme ist folgendermaßen aufgebaut: In Abschnitt II bietet sie einen kurzen Überblick über Vorgehensweisen der Internetdiensteanbieter beim Filtern. In Abschnitt III wird der EU-Rechtsrahmen für Netzneutralität dargestellt. In Abschnitt IV folgen dann eine technische Beschreibung sowie eine Bewertung der Auswirkungen der einzelnen Techniken auf den Schutz der Privatsphäre. In Abschnitt V werden praktische Einzelheiten der Anwendung des derzeitigen EU-Rahmens für Datenschutz und Schutz der Privatsphäre analysiert. Gestützt auf diese Analyse werden dann in Abschnitt VI Vorschläge für weitere politische Entwicklungen formuliert und die Bereiche aufgeführt, in denen unter Umständen eine Klarstellung und Verbesserung des Rechtsrahmens erforderlich ist. Abschnitt VII enthält die Schlussfolgerungen.

II. **NETZNEUTRALITÄT UND DATENVERKEHRSSTEUERUNG**

Zunehmender Einsatz von Datenverkehrssteuerung

11. Bisher haben Internetdiensteanbieter den Datenverkehr nur unter außergewöhnlichen Umständen überwacht und beeinflusst. So haben Internetdiensteanbieter beispielsweise Untersuchungstechniken angewandt und Datenströme beschränkt, um die Sicherheit des Netzes zu erhalten, z. B. zur Virenbekämpfung. Generell kann man also sagen, dass sich das Internet während seines Wachstums ein hohes Maß an Neutralität bewahrt hat.

12. In den letzten Jahren haben einige Internetdiensteanbieter jedoch ein Interesse an einer Steuerung des Datenverkehrs bekundet, um differenzieren und bestimmte Maßnahmen anwenden zu können, beispielsweise bestimmte Dienste zu sperren oder anderen Diensten Vorrang einzuräumen. Diese Vorgehensweise wird gelegentlich als „Datenverkehrssteuerung" (*traffic management policies*) bezeichnet ([9]).

13. Es gibt eine Vielzahl von Gründen für Internetdienstanbieter, den Datenverkehr steuern und differenzieren zu wollen. So kann die Datenverkehrssteuerung den Internetdiensteanbietern beispielsweise dabei helfen, den Datenverkehr in Zeiten extrem hohen Verkehrsaufkommens zu steuern, z. B. durch Bevorzugung eines bestimmten zeitabhängigen Verkehrs wie Video-Streaming und Herabstufung anderer Verkehrsarten wie P2P, die weniger zeitabhängig sein mögen. ([10]) Datenverkehrssteuerung kann für die Internetdiensteanbieter darüber hinaus potenzielle Einnahmen bedeuten, die aus verschiedenen Quellen stammen können. Auf der einen Seite könnten Internetdiensteanbieter Gebühren von den Anbietern von Inhaltsdiensten, deren Dienste eine größere Bandbreite erfordern, erheben und ihnen im Gegenzug Vorrang (und damit Geschwindigkeit) einräumen. Das würde bedeuten, dass der Zugang zu einem bestimmten Dienst, beispielsweise einem Dienst, der Video-on-Demand anbietet, schneller wäre als der Zugang zu einem ähnlichen Dienst, der sich nicht für die Hochgeschwindigkeitsübermittlung angemeldet hat. Einkünfte könnten auch von Abonnenten stammen, die bereit wären, höhere (oder niedrigere) Gebühren für bestimmte Arten differenzierter Abonnements zu zahlen. So könnte zum Beispiel ein Abonnement ohne Zugang zu P2P kostengünstiger als ein unbegrenzter Zugang sein.

14. Aber nicht nur die Internetdienstanbieter selbst haben Gründe für den Einsatz der Datenverkehrssteuerung, auch andere Akteure könnten Interesse an einer Datenverkehrssteuerung durch die Internetdienstanbieter haben. Wenn Internetdienstanbieter ihre Netze steuern und die Inhalte überwachen, die über ihre Einrichtungen laufen, könnten sie zunehmend in der Lage sein, mutmaßliche ungesetzliche Nutzung wie Verstöße gegen das Urheberrecht oder pornografische Nutzung zu entdecken.

([9]) Siehe beispielsweise den OFCOM-Bericht „Site blocking to reduce online copyright infringement", angenommen am 27. Mai 2011, abrufbar unter: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Einige Internetdiensteanbieter setzen bereits in ihren Netzen zur Datenverkehrssteuerung und zu anderen Zwecken Datenpaketüberprüfungssysteme (DPI) ein; daher gehen wir davon aus, dass sie einsetzbar sind, auch wenn dies außerordentlich komplex wäre und hohe Kosten für die mit sich brächte, die solche Dienste noch nicht betreiben. Es wäre also denkbar, dass in Anbetracht des erheblichen Investitionsbedarfs kurz- bis mittelfristig DPI nur von größeren Internetdiensteanbietern eingesetzt werden kann".

([10]) Die Qualität von Echtzeit-Anwendungen wie Video-Streaming ist unter anderem von der Latenz abhängig, also von der Verzögerung aufgrund von Engpässen im Netz.

Weitere wichtige Aspekte einschließlich Datenschutz und Schutz der Privatsphäre

15. Dieser Trend hat eine Debatte über die Legitimität dieser Art von Vorgehensweisen und insbesondere darüber ausgelöst, ob spezifische Verpflichtungen bezüglich der Netzneutralität gesetzlich näher festgelegt werden sollten.

16. Ein zunehmender Einsatz der Datenverkehrssteuerung durch Internetdiensteanbieter könnte den Zugang zu Informationen einschränken. Sollte diese Praxis um sich greifen, und sollte es für die Nutzer nicht mehr möglich (oder sehr teuer) werden, in vollem Umfang Zugang zum Internet zu bekommen, wie wir es kennen, würde dies den Zugang zu Informationen und die Fähigkeit des Nutzers gefährden, mit den Anwendungen oder Diensten seiner Wahl die Inhalte zu versenden und zu empfangen, die er möchte. Mit einem rechtlich verbindlichen Grundsatz der Netzneutralität ließe sich dieses Problem umgehen.

17. Damit kommt der EDSB zu den Auswirkungen der Datenverkehrssteuerung durch Internetdienstanbieter auf den Datenschutz und den Schutz der Privatsphäre. Es geht ihm vor allem um Folgendes:

— Wenn Internetdiensteanbieter Verkehrsdaten allein zu dem Zweck verarbeiten, den Datenstrom vom Sender zum Empfänger zu leiten, betreiben sie im Allgemeinen nur eine beschränkte Verarbeitung personenbezogener Daten ([11]). So wie die Post die Angaben auf einem Briefumschlag verarbeitet, verarbeitet der Internetdiensteanbieter die Daten, die er für die Übermittlung der Daten an den Empfänger benötigt. Dies steht nicht im Widerspruch zu den rechtlichen Anforderungen des Datenschutzes, des Schutzes der Privatsphäre und der Vertraulichkeit des Datenverkehrs.

— Wenn allerdings Internetdiensteanbieter Daten untersuchen, um jeden Datenfluss für sich zu behandeln und besondere Maßnahmen anzuwenden, die sich auf betroffene Personen nachteilig auswirken könnten, dann hat dies deutlichere Auswirkungen. Je nach den Gegebenheiten des Einzelfalls und je nach Art der durchgeführten Analyse kann die Verarbeitung einen massiven Eingriff in die Privatsphäre einer Person und ihre personenbezogenen Daten bedeuten. Dies gilt umso mehr, wenn die Steuerungsmaßnahmen den Inhalt der Internetverbindungen der betroffenen Person einschließlich gesendeter und empfangener E-Mails, besuchter Websites, herunter- oder hochgeladener Dateien usw. enthüllen.

III. ÜBERBLICK ÜBER DEN RECHTSRAHMEN DER EU ZUR NETZNEUTRALITÄT UND KÜNFTIGE POLITISCHE ENTWICKLUNGEN

III.1 Kurzdarstellung des Rechtsrahmens

18. Bis 2009 enthielten Rechtstexte der EU keine Bestimmungen, die Internetdiensteanbietern ausdrücklich ein Filtern oder Sperren oder Erheben von Extragebühren von Abonnenten für den Zugang zu Diensten verboten. Sie enthielten aber auch keine Bestimmungen, die diese Vorgehensweisen ausdrücklich billigten. Bis zu einem gewissen Grad war die Lage also unklar.

19. Das Telekom-Paket von 2009 brachte insofern eine Änderung mit sich, als es Bestimmungen enthielt, die für ein offenes Internet plädierten. So müssen beispielsweise nach Artikel 8 Absatz 4 der Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie") die nationalen Regulierungsbehörden die Endnutzer in die Lage versetzen, Informationen abzurufen oder beliebige Anwendungen und Dienste zu nutzen ([12]). Diese Vorschrift gilt für das Netz insgesamt, nicht nur für einzelne Anbieter. Auch im jüngsten Entwurf der Schlussfolgerungen des Rates wurde unterstrichen, wie notwendig es ist, die Offenheit des Internets zu erhalten ([13]).

([11]) Ausgeschlossen hiervon sind Vorgänge, mit denen die Sicherheit des Netzes gesteigert und schädlicher Datenverkehr ermittelt werden soll, sowie Vorgänge, die für Rechnungsstellung und Vernetzung erforderlich sind. Ausgeschlossen sind ferner Verpflichtungen nach der 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 verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105 vom 13.4.2006, S. 54) („Richtlinie über die Vorratsdatenspeicherung").

([12]) Richtlinie 2002/21/EG vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, geändert durch die Richtlinie 2009/140/EG und die Verordnung (EG) Nr. 544/2009 (ABl. L 337 vom 18.12.2009, S. 37).

([13]) Unter Punkt 3e anerkennt der Rat Folgendes: „Die Notwendigkeit, die Offenheit des Internets zu erhalten und gleichzeitig zu gewährleisten, dass es qualitativ hochwertige Dienste in einem Rahmen bereitstellen kann, der die Grundrechte wie die Meinungsfreiheit und die unternehmerische Freiheit achtet", und unter Punkt 8d fordert er die Mitgliedstaaten auf, „den offenen und neutralen Charakter des Internets als ihr politisches Ziel zu fördern".

20. Die Universaldienstrichtlinie ([14]) enthält konkretere Verpflichtungen. Artikel 20 und 21 legen Transparenzanforderungen für Beschränkungen des Zugangs zu und/oder der Nutzung von Diensten und Anwendungen fest. Gefordert wird dort auch ein Mindestniveau der Dienstqualität.

21. Bezüglich Vorgehensweisen von Internetdienstanbietern, die die Untersuchung des Datenverkehrs von Personen zur Folge haben, unterstreicht Erwägungsgrund 28 der Richtlinie zur Änderung der Universaldienstrichtlinie und der Datenschutzrichtlinie für die elektronische Kommunikation ([15]): „Je nach verwendeter Technologie und der Art der Einschränkungen kann für diese Einschränkungen die Einwilligung der Nutzer gemäß der Datenschutzrichtlinie für die elektronische Kommunikation erforderlich sein". Erwägungsgrund 28 verweist also noch einmal auf das Erfordernis der Einwilligung gemäß Artikel 5 Absatz 1 der Datenschutzrichtlinie für die elektronische Kommunikation bei allen Einschränkungen aufgrund der Überwachung des Datenverkehrs. Weiter unten wird in Abschnitt IV auf die Anwendung von Artikel 5 Absatz 1 sowie den allgemeinen Rechtsrahmen für den Datenschutz und den Schutz der Privatsphäre näher eingegangen.

22. Schließlich sind nach Artikel 22 Absatz 3 der Universaldienstrichtlinie die nationalen Regulierungsbehörden nunmehr befugt, erforderlichenfalls Mindestanforderungen an die Dienstqualität der Internetdiensteanbieter festzulegen und eine Behinderung oder Verlangsamung des Datenverkehrs in den öffentlichen Netzen zu verhindern.

23. Diese Ausführungen bedeuten, dass auf EU-Ebene weitgehend ein offenes Internet angestrebt wird (siehe Artikel 8 Absatz 4 der Rahmenrichtlinie). Dieses politische Ziel, das sich auf das Netz in seiner Gesamtheit bezieht, ist jedoch nicht unmittelbar mit Verboten oder Verpflichtungen einzelner Internetdiensteanbieter verknüpft. Mit anderen Worten: Ein Internetdiensteanbieter könnte Datenverkehrssteuerung betreiben, also unter Umständen den Zugang zu bestimmten Anwendungen ausschließen, solange er die Endnutzer umfassend informiert und diese ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage ihre Einwilligung hierzu erteilt haben.

24. Je nach Mitgliedstaat mag die Lage unterschiedlich sein. In manchen Mitgliedstaaten können Internetdiensteanbieter unter bestimmten Voraussetzungen Datenverkehrssteuerung betreiben, um beispielsweise (als Bestandteil eines günstigeren Internetabonnements) Anwendungen wie VoIP zu sperren, sofern die betroffenen Personen hierzu ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage ihre Einwilligung gegeben haben. Andere Mitgliedstaaten haben sich dafür entschieden, den Grundsatz der Netzneutralität zu stärken. So verabschiedete beispielsweise im Juli 2011 das niederländische Parlament ein Gesetz, das Anbietern generell verbietet, Anwendungen oder Dienste im Internet (wie VoIP) zu behindern oder zu verlangsamen, sofern dies nicht erforderlich ist, um die Auswirkungen von Engpässen zu mindern, aus Integritäts- oder Sicherheitsgründen, zur Bekämpfung von Spam oder aufgrund eines gerichtlichen Beschlusses ([16]).

III.2 **Die Mitteilung über Netzneutralität**

25. In ihrer Mitteilung zur Netzneutralität ([17]) kam die Europäische Kommission zu dem Schluss, dass die Lage beim Thema Netzneutralität der Überwachung und weiteren Analyse bedarf. Ihr Vorgehen wurde als „Politik des Abwartens" bezeichnet, bevor weitere regulatorische Schritte in Erwägung gezogen werden.

([14]) Richtlinie 2002/22/EG, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (ABl. L 337 vom 18.12.2009, S. 11). Vergleiche auch Artikel 1 Absatz 3, dem zufolge die Richtlinie Internetdiensteanbietern weder Bedingungen vorschreibt, die den Zugang zu und/oder die Nutzung von Diensten und Anwendungen durch die Endnutzer einschränken, soweit dies nach nationalem Recht zulässig ist und im Einklang mit dem Gemeinschaftsrecht steht, noch verbietet sie diese, begründet jedoch eine Verpflichtung zur Bereitstellung von Informationen über solche Bedingungen.

([15]) Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

([16]) Der Änderungsantrag im niederländischen Original kann eingesehen werden unter: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Die in der Presse genannten Gründe für diese politische Option hatten nichts mit Erwägungen im Zusammenhang mit dem Datenschutz oder den Schutz der Privatsphäre zu tun, sondern eher mit der Sorge, dass Nutzern der Zugang zu Informationen verwehrt oder nur in eingeschränktem Umfang gewährt wird. Hauptanlass für diesen Änderungsantrag scheint also die Problematik des Zugangs zu Informationen gewesen zu sein.

([17]) Vgl. Fußnote 4.

26. In der Mitteilung räumte die Kommission ein, dass alle Maßnahmen und weiteren regulatorischen Schritte im Hinblick auf Datenschutz und Schutz der Privatsphäre gründlich zu prüfen sind. Auch in dem Entwurf der Schlussfolgerungen des Rates werden die anstehenden Probleme beim Datenschutz und beim Schutz der Privatsphäre angesprochen ([18]).

27. Aus der Perspektive des Datenschutzes und des Schutzes der Privatsphäre wäre der Frage nachzugehen, ob eine Politik des Abwartens hier ausreicht. Zwar sieht der Rahmen für den Datenschutz und den Schutz der Privatsphäre gegenwärtig einige Garantien insbesondere mit Hilfe des Grundsatzes der Vertraulichkeit des Datenverkehrs vor, doch sollte die Einhaltung dieser Vorschriften besonders genau überwacht und sollten Leitlinien zu diversen Aspekten herausgegeben werden, die nicht besonders klar sind. Außerdem sollten Überlegungen dazu angestellt werden, wie der Rahmen im Lichte der technologischen Entwicklungen klarer gestaltet und weiter verbessert werden kann. Sollte die Überwachung ergeben, dass sich der Markt in Richtung einer massiven Steuerung des Datenverkehrs in Echtzeit entwickelt und damit Probleme mit der Einhaltung des Rahmens entstehen, werden gesetzgeberische Maßnahmen erforderlich. Konkrete Anregungen hierzu finden sich in Abschnitt VI.

IV. **TECHNISCHER HINTERGRUND UND DAMIT ZUSAMMENHÄNGENDE AUSWIRKUNGEN AUF DEN SCHUTZ DER PRIVATSPHÄRE UND DEN DATENSCHUTZ**

28. Vor einem tieferen Einstieg in das Thema soll an dieser Stelle ein kurzer Überblick über die Untersuchungstechniken gegeben werden, mit denen Internetdienstanbieter Datenverkehrssteuerung betreiben könnten, und soll geschildert werden, wie sich dies auf den Grundsatz der Netzneutralität auswirken könnte. Die Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz variieren stark je nach verwendeter/verwendeten Technik(en). Dieses technische Hintergrundwissen ist für das Verständnis und die ordnungsgemäße Anwendung des in Abschnitt V beschriebenen Datenschutzrahmens erforderlich. Es sei jedoch darauf hingewiesen, dass sich in diesem komplexen Bereich die Dinge ständig ändern. Die folgende Beschreibung erhebt daher keinen Anspruch auf Vollständigkeit und völlige Aktualität; sie soll vielmehr technische Informationen liefern, die für das Verständnis der rechtlichen Argumentation unerlässlich sind.

IV.1 **Datenübermittlung über das Internet: Grundlagen**

29. Wenn ein Nutzer Daten über das Internet versendet, werden die Daten in Pakete aufgeteilt. Diese Pakete werden über das Internet vom Sender an den Empfänger übermittelt. Jedes Paket enthält unter anderem Angaben zur Quelle und zum Ziel. Darüber hinaus können Internetdiensteanbieter diese Pakete in weitere Schichten und Protokolle ([19]), einbetten, die zur Steuerung der verschiedenen Verkehrsströme innerhalb des Netzes des Anbieters verwendet werden.

30. Noch einmal zurück zu dem Vergleich mit einem Brief: Die Verwendung eines Netzwerkprotokolls entspricht dem Einlegen des Briefes in einen Umschlag mit einer Empfängeradresse, die von der Post gelesen wird, worauf der Brief von der Post zugestellt werden kann. Die Post kann intern weitere Protokolle verwenden, damit alle Umschläge weitergeleitet werden; das Ziel besteht darin, dass jeder Umschlag seinen Bestimmungsort in der vom Absender verfassten Form erreicht. Bleiben wir noch ein wenig bei diesem Vergleich: Jedes Datenpaket umfasst zwei Teile, nämlich zunächst die *IP payload* mit dem Inhalt der Mitteilung — das entspräche dem Schreiben. Dieser Teil enthält Informationen, die nur für den Empfänger bestimmt sind. Der zweite Teil des Pakets ist der so genannte *IP header*, der unter anderem die Adresse des Empfängers und des Senders enthält und damit dem Umschlag entspräche. Der IP Header erlaubt dem Internetdienstanbieter und anderen zwischengeschalteten Stellen, die Payload von der Quelladresse zur Zieladresse zu befördern.

31. Internetdiensteanbieter und andere zwischengeschaltete Stellen sorgen dafür, dass IP-Pakete über Knoten durch das Netz reisen, an denen die IP Header-Daten gelesen, mit Routing-Tabellen abgeglichen und an den nächsten Knoten auf dem Weg zum Bestimmungsort geschickt werden. Dieser Prozess läuft über

([18]) So stellt der Rat unter Punkt 4e fest: „Das Vorhandensein einiger Bedenken, vorwiegend von Verbrauchern und Datenschutzbehörden, bezüglich des Schutzes personenbezogener Daten".

([19]) Wie in Abschnitt IV.2 näher beschrieben, kodieren solche Protokolle die zu übermittelnden Daten in einer vereinbarten Weise von Endpunkt zu Endpunkt, damit die am Datenverkehr Beteiligten einander verstehen, wie HTTP, FTP usw.

das Netz ab, und zwar nach einem „best effort memoryless"-Ansatz, da alle an einem Knoten ankommenden Pakete gleich behandelt werden. Nach ihrer Weiterleitung an den nächsten Knoten brauchen keine Daten mehr im Router gespeichert zu werden ([20]).

IV.2 **Untersuchungstechniken**

32. Wie bereits erläutert, lesen Internetdienstanbieter IP Header zu dem Zweck, sie an ihr Ziel weiterzuleiten. Wie jedoch vorstehend ausgeführt, kann die Verkehrsanalyse (anhand von IP Header und IP Payload) auch zu anderen Zwecken und mit anderen Technologien vorgenommen werden. Neue Tendenzen können beispielsweise die Verlangsamung bestimmter von den Nutzern genutzter Anwendungen wie P2P oder auch die Erhöhung der Verkehrsgeschwindigkeit bei bestimmten Diensten wie Video-on-Demand für Premium-Abonnenten umfassen. *Technisch* wird mit allen Untersuchungstechniken eine Untersuchung der Pakete durchgeführt, doch bedeuten sie unterschiedlich starke Eingriffe in die Privatsphäre. Es gibt zwei Hauptkategorien von Untersuchungstechniken. Die eine stützt sich nur auf den IP Header, die andere auch auf die IP Payload.

Gestützt auf die IP Header-Daten. Bei der Untersuchung eines IP Paket-Headers werden einige Felder freigelegt, die dem Internetdienstanbieter die Möglichkeiten bieten, besondere Maßnahmen zur Verkehrssteuerung durchzuführen. Diese allein auf der Untersuchung von IP Headern basierenden Techniken verarbeiten Daten, die grundsätzlich für das Routing gedacht sind, für einen anderen Zweck (nämlich die Differenzierung des Datenverkehrs). Nach einem Blick auf die IP-Adresse der Quelle kann der Internetdiensteanbieter diese mit einem konkreten Abonnenten verknüpfen und entsprechende Maßnahmen einleiten, also z. B. das Paket über eine schnellere oder langsamere Verbindung weiterleiten. Aber auch ein Blick auf die IP-Adresse des Ziels gibt dem Internetdiensteanbieter die Möglichkeit, bestimmte Maßnahmen durchzuführen, wie beispielsweise das Sperren oder Filtern des Zugangs zu bestimmten Websites.

Gestützt auf eine gründliche Untersuchung. Bei der so genannten *Deep Packet Inspection* hat der Internetdiensteanbieter Zugriff auf Daten, die eigentlich nur an den Empfänger der Nachricht gerichtet sind. Wenn wir noch einmal das Beispiel mit dem Brief aufgreifen, dann entspricht dies dem Öffnen des Umschlags und dem Lesen des darin enthaltenen Briefes zwecks einer Analyse des Inhalts der (in den IP-Paketen eingeschlossenen) Nachricht mit dem Ziel, eine bestimmte Netzwerkmaßnahme anzuwenden. Es bestehen verschiedene Möglichkeiten für die Durchführung der Untersuchung, die jeweils unterschiedliche Bedrohungen für die betroffene Person darstellen.

— *Deep Packet Inspection auf der Grundlage der Analyse von Protokollen und von statistischen Aufzeichnungen*. Neben dem IP-Protokoll, das dafür gedacht ist, die Daten über das Internet zu übermitteln, gibt es noch weitere Protokolle, die nach einer Vereinbarung die zu übermittelnden Daten kodieren (Beförderung, Sitzung, Präsentation und Anwendung usw.). Mit diesen Protokollen soll gewährleistet werden, dass die an der Kommunikation Beteiligten einander verstehen. So gibt es beispielsweise einige Protokolle für Web-Browsing ([21]), andere für die Übertragung von Dateien ([22]) usw. Untersuchungstechniken, die auf der Untersuchung von Protokollen fußen und mit statistischen Analysen kombiniert werden, haben daher das Ziel, nach besonderen Mustern oder Fingerabdrücken zu suchen, die bestimmen, welche Protokolle vorhanden sind ([23]). Mit Hilfe dieser Untersuchungstechniken erfährt der Internetdiensteanbieter, um welche Art von Kommunikation es geht (E-Mail, Web-Browsing, Hochladen von Dateien), und kann in manchen Fällen den jeweils verwendeten Dienst oder die jeweils verwendete Anwendung identifizieren, wie bei einigen VoIP-Kommunikationen, bei denen die verwendeten Protokolle für einen konkreten Verkäufer oder Diensteanbieter typisch sind. Allein das Wissen um die Art der Kommunikation erlaubt dem Internetdiensteanbieter, konkrete Verkehrssteuerungsmaßnahmen vorzunehmen. So kann er zum Beispiel den Web-Verkehr sperren. Es kann aber auch der erste Schritt in Richtung der Möglichkeit für den Internetdienstanbieter sein, weitere Analysen vorzunehmen, die umfassenden Zugriff auf die Metadaten und den Inhalt der Kommunikation erfordern.

([20]) Dessen ungeachtet verwendet die Internet-Netzausrüstung Routing-Protokolle, die Aktivität vermerken, Verkehrsstatistiken verarbeiten und mit anderen Netzgeräten Informationen austauschen, um für die Weiterleitung von IP-Paketen den effizientesten Pfad zu finden. Ist z. B. eine Verbindung überlastet oder zusammengebrochen und erhält ein Router diese Information, aktualisiert er seine Routing-Tabelle mit einer Alternative, die diese Verbindung nicht benutzt. Es sei auch auf die Erhebung und Verarbeitung hingewiesen, die in manchen Fällen zu Rechnungsstellungszwecken oder sogar im Einklang mit den Anforderungen der Richtlinie über die Vorratsdatenspeicherung erfolgt.

([21]) HTTP — Hypertext transfer protocol — oder HTML — Hypertext Markup Language.

([22]) FTP — File transfer protocol.

([23]) Für die Identifizierung der verwendeten Protokolle gibt es verschiedene Methoden. So kann man beispielsweise besondere Felder in inneren Protokollen durchsuchen, um die für die Herstellung der Verbindung verwendeten Ports zu identifizieren. Eine statistische Charakterisierung eines Datenflusses lässt sich auch aus der Analyse einiger besonderer Felder ableiten, einer Korrelation der Felder, die gleichzeitig zwischen zwei IP-Adressen benutzt wurden.

— *Deep Packet Inspection auf der Grundlage der Analyse des Inhalts der Kommunikation.* Schließlich ist es auch möglich, die Metadaten ([24]) und den Inhalt der Kommunikation zu untersuchen. Diese Technik besteht aus dem Abfangen aller IP-Pakete, die Bestandteil des ursprünglichen Datenstromes waren, so dass der Originalinhalt der Kommunikation in vollem Umfang rekonstruiert und analysiert werden kann. Zur Aufdeckung schädlicher oder illegaler Inhalte wie Viren, Kinderpornographie usw. muss zum Beispiel der Inhalt selbst rekonstruiert werden, damit er analysiert werden kann. Es sei darauf hingewiesen, dass mitunter die Kommunikation von den Beteiligten absichtlich Ende-zu-Ende verschlüsselt wird; damit kann der Internetdiensteanbieter dann keine Analyse des Inhalts der Kommunikation vornehmen.

IV.3 **Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz**

33. Untersuchungstechniken, die sich auf IP Header stützen, und insbesondere die Techniken, die auf der Paket-Untersuchung fußen, beinhalten die Überwachung und das Filtern dieser Daten und haben ernstzunehmende Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz. Sie können auch mit dem Recht auf Vertraulichkeit der Kommunikation in Konflikt geraten.

34. Schon der Einblick in die Kommunikation einer Person wirkt sich ernsthaft auf den Schutz der Privatsphäre und den Datenschutz aus. Das Problem ist jedoch noch umfassender, denn je nach den mit der Überwachung und dem Abfangen verfolgten Zielen nehmen die Auswirkungen auf den Schutz der Privatsphäre zu. Es ist nämlich nicht das Gleiche, Kommunikationen beispielsweise nur zu untersuchen, um zu gewährleisten, dass das System gut funktioniert, und Kommunikationen zu untersuchen, um dann Maßnahmen durchzuführen, die sich auf die betroffene Person auswirken könnten. Dienen Verkehrs- und Auswahlmaßnahmen allein dazu, eine Überlastung des Netzes zu vermeiden, dürften normalerweise keine größeren Auswirkungen auf die Privatsphäre einer Person entstehen. Maßnahmen zur Datenverkehrssteuerung können jedoch darauf abheben, bestimmte Inhalte zu sperren oder die Kommunikation beispielsweise durch verhaltensorientierte Werbung zu beeinflussen. In diesen Fällen sind deutliche Effekte auf die Privatsphäre zu spüren. Noch bedenklicher wird diese Frage, wenn man bedenkt, dass diese Art von Informationen nicht nur über eine kleine Gruppe von Personen gesammelt würde, sondern stattdessen allgemein, über alle Kunden eines Internetdienstanbieters ([25]). Sollten alle Internetdienstanbieter Filtertechniken anwenden, könnte dies zu einer allgemeinen Überwachung der Internetnutzung führen. Befasst man sich außerdem näher mit der Art von Daten, die verarbeitet werden, bestehen offensichtlich große Risiken für die Privatsphäre, da ein Großteil der erhobenen Daten äußerst sensibel sein dürfte und nach der Erhebung den Internetdiensteanbietern und denen, die Daten von ihnen erhalten möchten, zur Verfügung steht. Des Weiteren könnten die Daten auch kommerziell äußerst wertvoll sein. Allein das birgt schon ein großes Risiko der Zweckentfremdung in sich, wenn nämlich die ursprüngliche Zweckbestimmung leicht in eine kommerzielle oder anderweitige Nutzung der erhobenen Daten übergehen könnte.

35. Die korrekte Anwendung von Überwachungs- und Untersuchungstechniken hat im Einklang mit den anzuwendenden Garantien für den Datenschutz und den Schutz der Privatsphäre zu erfolgen, in denen genau abgegrenzt ist, was unter welchen Umständen gemacht werden darf. Nachstehend folgt ein Überblick über die Garantien, die nach dem derzeitigen EU-Rechtsrahmen für den Datenschutz und den Schutz der Privatsphäre anzuwenden sind.

V. **ANWENDUNG DES EU-RECHTSRAHMENS FÜR DEN SCHUTZ DER PRIVATSPHÄRE UND DEN DATENSCHUTZ**

36. Der EU-Datenschutzrahmen ist technikneutral; somit regelt er keine besonderen Untersuchungstechniken wie die vorstehend beschriebenen. Die Datenschutzrichtlinie für elektronische Kommunikation regelt den Datenschutz bei der Erbringung elektronischer Kommunikationsdienste in öffentlichen

([24]) Jedes Protokoll verfügt in seinem Header über einige Felder, die weitere informelle Informationen zur übertragenen Nachricht liefern. Den Inhalt dieser Felder könnte man als die Metadaten der Nachricht bezeichnen. Als Beispiel für solche Felder sei die Nummer des verwendeten Ports genannt; lautet diese Zahl 80, ist es sehr wahrscheinlich, dass es sich bei der Kommunikation um Web-Browsing handelt.

([25]) Natürlich können nicht nur Internetdienstanbieter Nutzer verfolgen. Auch Werbe-Netzwerkbetreiber können mit Hilfe von Cookies Dritter Nutzer über Websites hinweg verfolgen. Siehe hierzu zum Beispiel einen vor kurzem erschienenen wissenschaftlichen Artikel, der zeigt, dass Google auf 97 von 100 Websites präsent ist; das bedeutet, dass Google Nutzer, die Cookies Dritter nicht abgeschaltet haben, beim Browsen auf diesen beliebten Websites verfolgen kann. Siehe: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (July 29, 2011). Abrufbar bei SSRN: http://ssrn.com/abstract=1898390. Mit der Verfolgung von Nutzern mit Hilfe von Cookies Dritter hat sich auch die Artikel 29-Datenschutzgruppe befasst. Siehe Stellungnahme 2/2010 über Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010 (WP 171).

Netzen (in der Regel Internetzugang und Telefondienste) ([26]), die Datenschutzrichtlinie regelt die Verarbeitung von Daten allgemein. Alles in allem sind in diesem Rechtrahmen die Verpflichtungen für Internetdiensteanbieter festgelegt, die Verkehrs- und Kommunikationsdaten verarbeiten und überwachen.

V.1 **Rechtsgrundlage für die Verarbeitung von Verkehrs- und Inhaltsdaten**

37. Nach den Datenschutzvorschriften bedarf die Verarbeitung personenbezogener Daten, in diesem Fall also die Verarbeitung von Verkehrs- und Kommunikationsdaten, einer angemessenen Rechtsgrundlage. Neben dieser allgemeinen Anforderung können in bestimmten Fällen noch spezifische Anforderungen gelten.

38. Im vorliegenden Fall handelt es sich bei den durch die Internetdienstanbieter verarbeiteten Daten um Verkehrsdaten und Kommunikationsinhalte. Kommunikationsinhalte und Verkehrsdaten sind durch das Recht auf Achtung der Korrespondenz geschützt, das zum einen in Artikel 8 EMRK und zum anderen in den Artikeln 7 und 8 der Charta verankert ist. Weiter fordert Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation, der den Titel „Vertraulichkeit der Kommunikation" trägt, die Mitgliedstaaten auf, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicherzustellen. Daneben sieht Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation vor, dass die Verarbeitung von Verkehrs- und Inhaltsdaten durch Internetdiensteanbieter unter bestimmten Voraussetzungen und mit der Einwilligung der Nutzer zulässig sein kann. Hierzu wird dort das „Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind" untersagt. Hierauf wird weiter unten näher eingegangen.

39. Neben der Einwilligung der betroffenen Nutzer sieht die Datenschutzrichtlinie für elektronische Kommunikation noch weitere Gründe vor, aus denen eine Verarbeitung von Verkehrs- und Kommunikationsdaten durch Internetdiensteanbieter rechtmäßig sein kann. Die einschlägigen Rechtsgrundlagen für die Verarbeitung in diesem Fall sind i) die Bereitstellung des Dienstes; ii) die Gewährleistung der Sicherheit des Dienstes und iii) die Verringerung der Überlastung auf ein Mindestmaß. Weitere mögliche Gründe, aus denen auf Verkehrs- und Kommunikationsdaten fußende Steuerungsmaßnahmen rechtmäßig sein könnten, werden weiter unten unter Punkt iv diskutiert.

i) Rechtsgrundlage für die Bereitstellung des Dienstes

40. Wie in Abschnitt IV dargestellt, verarbeiten Internetdiensteanbieter Daten aus IP Headern zu dem Zweck, die einzelnen IP-Pakete zu ihrem Ziel weiterzuleiten. Gemäß Artikel 6 Absatz 1 und Artikel 6 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation ist die Verarbeitung von Verkehrsdaten für die Übertragung einer Nachricht zulässig. Somit dürfen Internetdienstanbieter die Daten verarbeiten, die für die Bereitstellung des Dienstes erforderlich sind.

ii) Rechtsgrundlage für die Gewährleistung der Sicherheit des Dienstes

41. Laut Artikel 4 der Datenschutzrichtlinie über elektronische Kommunikation ist ein Internetdienstanbieter generell verpflichtet, geeignete Maßnahmen zu ergreifen, um die Sicherheit seiner Dienste zu gewährleisten. Beim Herausfiltern von Viren kann die Verarbeitung von IP Headern und IP Payload erforderlich sein. Unter Berücksichtigung der Tatsache, dass Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation von Internetdiensteanbietern verlangt, die Sicherheit des Netzes zu gewährleisten, sind damit Untersuchungstechniken legitimiert, die auf IP Headern und Inhalt beruhen und allein dem Erreichen dieses Ziels dienen. In der Praxis bedeutet dies, dass innerhalb der durch den Grundsatz der Verhältnismäßigkeit abgesteckten Grenzen (siehe Abschnitt V.3) Internetdienstanbieter zur Virenbekämpfung und generell zur Gewährleistung der Sicherheit des Netzes Kommunikationsdaten überwachen und filtern dürfen ([27]).

([26]) Erwägungsgrund 10 der Datenschutzrichtlinie für elektronische Kommunikation lautet: „Im Bereich der elektronischen Kommunikation gilt die Richtlinie 95/46/EG vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen". Auch Erwägungsgrund 19 ist für die Einwilligung der betroffenen Person von Bedeutung: „Für die Zwecke dieser Richtlinie sollte die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff ‚Einwilligung der betroffenen Person'".

([27]) Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post, angenommen am 21. Februar 2006 (WP 118). In dieser Stellungnahme vertritt die Datenschutzgruppe die Ansicht, dass der Einsatz von Filtern für den Zweck von Artikel 4 mit Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation durchaus vereinbar sein kann.

iii) Rechtsgrundlage für die Verringerung der Auswirkungen der Überlastung auf ein Mindestmaß

42. Die Begründung für diese Rechtsgrundlage findet sich in Erwägungsgrund 22 der Datenschutzrichtlinie für elektronische Kommunikation, in dem das in Artikel 5 Absatz 1 formulierte Verbot der Speicherung von Nachrichten erläutert wird. Damit soll nicht jede automatische, einstweilige und vorübergehende Speicherung insoweit untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung erfolgt und als die Speicherung nicht länger erfolgt, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Kommunikation gewährleistet ist.

43. Bei einer Überlastung stellt sich die Frage, ob ein Internetdiensteanbieter beliebig Datenverkehr fallenlassen oder verzögern und eher Nachrichten verlangsamen darf, die nicht zeitabhängig sind, wie z. B. P2P oder E-Mail-Verkehr, und damit z. B. Telefonverkehr in annehmbarer Qualität ermöglicht.

44. In Anbetracht des gesamtgesellschaftlichen Interesses an der Gewährleistung eines nutzbaren Kommunikationsnetzes könnten die Internetdiensteanbieter argumentieren, dass die vorrangige Behandlung oder das Drosseln des Datenverkehrs zur Bewältigung von Engpässen eine legitime Maßnahme sei, die für die Bereitstellung eines angemessenen Dienstes erforderlich sei. Das bedeutet, dass es in diesen Fällen und zu diesem Zweck eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten gibt und eine ausdrückliche Einwilligung der Nutzer nicht erforderlich wäre.

45. Gleichzeitig sind die Möglichkeiten, auf diese Weise einzugreifen, allerdings nicht unbeschränkt. Falls Internetdienstanbieter Nachrichten untersuchen müssen, haben sie aus Gründen der Vertraulichkeit und unter strikter Anwendung des Grundsatzes der Verhältnismäßigkeit die am wenigsten in die Privatsphäre eindringende Methode zu wählen, die für diesen Zweck zur Verfügung steht (und dabei Deep Packet Inspection zu vermeiden), und sie dürfen diese Methode nur so lange anwenden, wie es für die Beseitigung der Überlastung erforderlich ist.

iv) Rechtsgrundlage für die Verarbeitung von Daten zu anderen Zwecken

46. Es kann vorkommen, dass Internetdienstanbieter Verkehrs- und Inhaltsdaten auch zu anderen Zwecken untersuchen möchten, beispielsweise, um gezielte Abonnements anzubieten (z. B. ein Abonnement, das Zugang zu P2P begrenzt, oder ein Abonnement, bei dem für bestimmte Anwendungen eine höhere Geschwindigkeit geboten wird). Die Untersuchung und weitere Nutzung von Verkehrs- und Kommunikationsdaten zu anderen Zwecken als der Bereitstellung des Dienstes oder der Gewährleistung der Sicherheit des Netzes oder des Abbaus einer Überlastung sind nur unter strengsten Bedingungen und im Einklang mit dem rechtlichen Rahmen zulässig.

47. Den rechtlichen Rahmen bildet im Wesentlichen Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation, der die Einwilligung der betroffenen Nutzer fordert, wenn es um das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten geht. In der Praxis bedeutet dies, dass die Einwilligung der an einer Kommunikation beteiligten Nutzer erforderlich ist, damit die Verarbeitung sowohl von Verkehrs- als auch Kommunikationsdaten gemäß Artikel 5 Absatz 1 rechtmäßig ist.

48. Wie bereits erläutert, stützen sich Untersuchungs- und Filtertechniken entweder auf IP Header, also Verkehrsdaten, oder auf eine Deep Packet Inspection, die auch die IP Payload umfasst und die Kommunikationsdaten bildet. Grundsätzlich wäre daher die Anwendung solcher Techniken zu anderen Zwecken als der Übertragung der Nachricht oder der Gewährleistung der Sicherheit untersagt, falls nicht aus einem rechtlichen Grund wie der Einwilligung die Verarbeitung rechtmäßig ist (Artikel 5 Absatz 1). Artikel 5 Absatz 1 würde beispielsweise greifen, wenn ein Internetdiensteanbieter beschließt, seinen Kunden den Internetzugang billiger anzubieten, wenn sie im Gegenzug verhaltensorientierte Werbung akzeptieren, wobei er Deep Packet Inspection und damit Kommunikationsdaten zu diesem Zweck einsetzen würde. Daher wäre gemäß Artikel 5 Absatz 1 eine echte, für den konkreten Fall und in Kenntnis der Sachlage erteilte Einwilligung erforderlich.

49. Darüber hinaus enthält Artikel 6 der Datenschutzrichtlinie für elektronische Kommunikation mit dem Titel „Verkehrsdaten“ bestimmte Vorschriften, die speziell für Verkehrsdaten gelten. Genauer gesagt sieht dieser

Artikel vor, dass der Internetdienstanbieter Verkehrsdaten verarbeiten kann, wenn der Nutzer eingewilligt hat, Dienste mit Zusatznutzen zu empfangen ([28]). In dieser Bestimmung wird das in Artikel 5 Absatz 1 vorgesehene Erfordernis der Einwilligung, sobald es um Verkehrsdaten geht, näher spezifiziert.

50. In der Praxis mag es nicht immer einfach zu bestimmen sein, in welchen Fällen zum Beispiel eine Einwilligung erforderlich ist und in welchen Fällen die Sicherheit des Netzes eine Verarbeitung rechtfertigt, insbesondere wenn die Untersuchungstechniken einen doppelten Zweck verfolgen (z. B. Vermeidung von Überlastung und Bereitstellung von Diensten mit Zusatznutzen). Es sollte darauf hingewiesen werden, dass die Einwilligung nicht einfach und immer bedeutet, dass Datenschutzgrundsätze eingehalten werden.

51. Es liegen nur wenige Erfahrungen mit der Anwendung des Rahmens und insbesondere mit den oben dargestellten Aspekten vor. In diesem Bereich sind weitere Leitlinien notwendig, wie in Abschnitt VI weiter ausgeführt wird. Darüber hinaus gibt es weitere wichtige Aspekte im Zusammenhang mit der Erteilung der Einwilligung, die besonderer Betrachtung bedürfen. Sie werden nachstehend beschrieben.

V.2 **Probleme im Zusammenhang mit der Erteilung der Einwilligung in Kenntnis der Sachlage als Rechtsgrundlage**

52. Die in Artikel 5 und 6 der Datenschutzrichtlinie für elektronische Kommunikation geforderte Einwilligung hat die gleiche Bedeutung wie die Einwilligung der betroffenen Person, wie sie in der Richtlinie 95/46/EG definiert und näher spezifiziert ist ([29]). Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie gilt als Einwilligung der betroffenen Person „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass sie betreffende personenbezogene Daten verarbeitet werden". Erst vor kurzem hat sich die Artikel 29-Datenschutzgruppe in ihrer Stellungnahme 15/2011 zur Definition von Einwilligung mit der Rolle der Einwilligung und den Bedingungen, die sie erfüllen muss, um gültig zu sein, befasst ([30]).

53. Internetdiensteanbieter, die eine Einwilligung fordern, um Verkehrs- und Inhaltsdaten untersuchen und filtern zu können, müssen daher dafür sorgen, dass die Einwilligung ohne Zwang und für den konkreten Fall gegeben wird, und es muss eine Willensbekundung in Kenntnis der Sachlage erfolgen, mit der die betroffene Person akzeptiert, dass sie betreffende personenbezogene Daten verarbeitet werden. Bestätigt wird diese Aussage in Erwägungsgrund 17 der Datenschutzrichtlinie für elektronische Kommunikation: „(…) Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website". Im Folgenden sind einige Beispiele dafür aufgeführt, was in diesem Zusammenhang unter einer Einwilligung zu verstehen ist, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben wird.

Einwilligung: ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage

54. *Einwilligung ohne Zwang*. Die Nutzer sollten keinerlei Zwang unterliegen, wenn sie eine Einwilligung im Zusammenhang mit dem Internet-Abonnement geben, das sie abschließen wollen.

55. Die Einwilligung der betroffenen Personen wäre nicht freiwillig, wenn sie einer Überwachung ihrer Kommunikationsdaten zustimmen müssten, um Zugang zu einem Kommunikationsdienst zu erhalten. Dies träfe noch mehr zu, wenn *alle* Anbieter auf einem bestimmten Markt Verkehrssteuerung zu Zwecken vornehmen wollten, die über die Gewährleistung der Sicherheit des Netzes hinausgingen. Es bliebe nur die Möglichkeit, überhaupt keinen Internetdienst zu abonnieren. Nachdem sich das Internet zu einem wesentlichen Instrument für berufliche wie private Zwecke entwickelt hat, ist der

([28]) Erwägungsgrund 18 der Richtlinie enthält eine Liste mit Beispielen von Diensten mit Zusatznutzen. Es ist jedoch unklar, ob Dienste, auf die Datenverkehrssteuerung angewandt wird, als Teil dieser Liste gedeutet werden können. Eine Datenverkehrssteuerung, mit der bestimmten Inhalten Vorrang eingeräumt werden soll, kann als Element zur Verbesserung der Qualität des Dienstes aufgefasst werden. Eine Datenverkehrssteuerung, die beispielsweise nur die Verarbeitung von IP Headern zur Folge hat und mit dem Ziel erfolgt, höherpreisige Dienste für Online-Spiele anzubieten, bei denen der der Datenverkehr von Online-Spielen des Nutzers im Netz vorrangig behandelt wird, könnte als Dienst mit Zusatznutzen betrachtet werden. Auf der anderen Seite steht noch überhaupt nicht fest, ob eine Datenverkehrssteuerung mit dem Ziel einer Drosselung bestimmter Verkehrsarten, wie z. B. ein Herunterstufen des P2P-Verkehrs, als solche gelten kann.

([29]) Vgl. Erwägungsgrund 17 und Artikel 2 Buchstabe f der Datenschutzrichtlinie für elektronische Kommunikation.

([30]) Angenommen am 13. Juli 2011 (WP 187).

Verzicht auf einen Vertrag mit einem Internetanbieter keine realistische Alternative. Die betroffenen Personen hätten folglich keine echte Wahl; sie könnten ihre Einwilligung also auch nicht ohne Zwang geben ([31]).

56. Nach Ansicht des EDSB sollten die Kommission und die nationalen Behörden unbedingt den Markt beobachten und vor allem darauf achten, ob diese Konstellation — also Anbieter, die Telekommunikationsdienste mit einer Überwachung der Kommunikation verknüpfen — sich durchsetzt. Die Anbieter sollten Alternativdienste anbieten, einschließlich eines Internetabonnements ohne Datenverkehrssteuerung, ohne jedoch dafür höhere Preise zu verlangen.

57. *Einwilligung für den konkreten Fall*. Einwilligung für den konkreten Fall bedeutet hier, dass Internetdiensteanbieter klar und eindeutig die Einwilligung zur Überwachung von Verkehrs- und Kommunikationsdaten einholen. Die Artikel 29-Datenschutzgruppe sagt hierzu: „Damit sie für den konkreten Fall ist, muss die Einwilligung verständlich sein: Sie sollte sich eindeutig und genau auf den Anwendungsbereich und die Folgen der Datenverarbeitung beziehen. Sie kann nicht für Verarbeitungsaktivitäten gelten, die in keinster Weise eingegrenzt sind. Das heißt mit anderen Worten, dass der Kontext, in dem die Einwilligung gilt, eingeschränkt ist". Eine Einwilligung für den konkreten Fall dürfte kaum erlangt werden, wenn die Einwilligung in die Untersuchung der Verkehrs- und Kommunikationsdaten mit der Gesamteinwilligung, einen Dienst zu abonnieren, „verknüpft" ist. Statt dessen sollte um die Einwilligung für den konkreten Fall mit gezielten Mitteln ersucht werden, wie mit einem eigenen Einwilligungsformular oder einem Feld, das eindeutig auf den Zweck der Überwachung hinweist (und nicht mit der Unterbringung dieser Informationen in den allgemeinen Vertragsbedingungen und der Aufforderung, den Vertrag unverändert zu unterschreiben).

58. *Einwilligung in voller Sachkenntnis*. Damit eine Einwilligung gültig ist, muss sie in voller Sachkenntnis gegeben worden sein. Das Erfordernis einer angemessenen Information im Vorfeld ergibt sich nicht nur aus der Datenschutzrichtlinie für elektronische Kommunikation und der Datenschutzrichtlinie, sondern auch aus den Artikeln 20 und 21 der Universaldienstrichtlinie, geändert durch die Richtlinie 2009/136/EG ([32]). Das Erfordernis der Information und Einwilligung wurde in Erwägungsgrund 28 der Richtlinie 2009/136/EG ausdrücklich bestätigt: „Die Nutzer sollten auf jeden Fall vom Diensteanbieter und/oder Netzbetreiber vollständig über mögliche Einschränkungsbedingungen und Grenzen bei der Nutzung der elektronischen Kommunikationsdienste informiert werden. Im Rahmen dieser Informationen sollten nach Wahl des Anbieters entweder die Art der betreffenden Inhalte, Anwendungen oder Dienste oder die Einzelanwendungen oder -dienste oder beides bestimmt werden." Weiter heißt es dort: „Je nach verwendeter Technologie und der Art der Einschränkungen kann für diese Einschränkungen die Einwilligung der Nutzer gemäß der Richtlinie 2002/58/EG erforderlich sein."

59. In Anbetracht der Komplexität dieser Überwachungstechniken ist die Vermittlung aussagekräftiger Vorabinformationen eine der Hauptvoraussetzungen für eine gültige Einwilligung. Die Verbraucher sollten so unterrichtet werden, dass sie begreifen, welche Informationen verarbeitet werden, wie sie verwendet werden, welche Auswirkungen auf die Erfahrung der Nutzer die Techniken haben und wie weit sie in die Privatsphäre eindringen.

60. Das bedeutet nicht nur, dass die Informationen selber für den durchschnittlichen Nutzer klar und verständlich sein müssen, sondern auch, dass sie für die betroffenen Personen gut sichtbar sein müssen, damit sie nicht übersehen werden.

61. *Willenserklärung*. Schließlich ist es nach dem geltenden rechtlichen Rahmen erforderlich, dass der Nutzer aktiv seine Einwilligung gibt. Eine stillschweigende Einwilligung entspräche nicht den Vorschriften. Dies bestätigt, dass es besonderer Methoden bedarf, um die Einwilligung einzuholen, aufgrund derer der Internetdiensteanbieter Verkehrs- und Kommunikationsdaten im Rahmen der Datenverkehrssteuerung untersuchen darf. In ihrer jüngst angenommenen Stellungnahme zum Thema Einwilligung unterstrich die Artikel 29-Datenschutzgruppe die Anforderung der Granularität der Einwilligung in Bezug auf die verschiedenen Elemente, die die Datenverarbeitung ausmachen.

([31]) Ein ähnlich gelagerter Fall ist PNR, bei dem es darum ging, ob die Einwilligung der Passagiere zur Übermittlung der Buchungsdaten an die US-Behörden gültig war. Die Datenschutzgruppe vertrat die Auffassung, dass die Einwilligung nicht ohne Zwang erfolgen kann, da die Fluggesellschaften die Daten vor dem Start des Flugzeugs übermitteln müssen und die Passagiere somit keine Wahl haben, wenn sie ihren Flug antreten möchten; Stellungnahme 6/2002 der Artikel 29-Datenschutzgruppe zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten.

([32]) Richtlinie 2009/136/EG vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (siehe Fußnote 15).

62. Man könnte nun folgendermaßen argumentieren: Wenn die an einer Kommunikation Beteiligten nicht möchten, dass Internetdiensteanbieter diese zu Zwecken der Datenverkehrssteuerung abfangen, können sie die Kommunikation immer noch verschlüsseln. In der Praxis könnte sich dieser Ansatz als hilfreich erweisen, doch erfordert er einiges an Aufwand und technischem Wissen und kann nicht mit einer Einwilligung gleichgesetzt werden, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben wurde. Aber auch der Einsatz von Verschlüsselungstechniken kann eine Nachricht nicht völlig vertraulich machen, da der Internetdiensteanbieter zumindest Zugriff auf die IP Header-Daten hat, damit er die Nachricht weiterleiten kann, und außerdem in der Lage ist, statistische Analysen vorzunehmen.

63. Gemäß Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation ist von den betroffenen Nutzern die Einwilligung einzuholen. Häufig ist der Nutzer mit dem Abonnenten identisch; dann kann die Einwilligung bei der Unterzeichnung des Abonnements des Telekommunikationsdienstes gegeben werden. In anderen Fällen, also auch, wenn mehr als eine Person beteiligt sind, muss die Einwilligung jedes einzelnen Nutzers eingeholt werden. Wie nachstehend dargestellt, kann dies zu praktischen Problemen führen.

Einwilligung aller betroffenen Nutzer

64. Laut Artikel 5 Absatz 1 ist eine Verarbeitung nur rechtmäßig, wenn der Nutzer seine Einwilligung gegeben hat. Die Einwilligung ist von *allen* an einer Kommunikation beteiligten *Nutzern* einzuholen. Grund dafür ist, dass von einer Nachricht in der Regel mindestens zwei Personen betroffen sind (Sender und Empfänger). Scannt ein Internetdiensteanbieter beispielsweise IP Payloads einer E-Mail, untersucht er Daten, die sowohl mit dem Sender als auch mit dem Empfänger der E-Mail zu tun haben.

65. Bei der Überwachung und dem Abfangen von Verkehr und Nachrichten (z. B. von Web-Verkehr) mag es für den Internetdienstanbieter ausreichen, die Einwilligung nur eines Nutzers einzuholen, nämlich des Abonnenten. Der Grund dafür ist, dass der andere an der Kommunikation Beteiligte, in diesem Fall die besuchte Website, nicht als „betroffener Nutzer" gilt ([33]). Komplizierter wird die Lage jedoch, wenn bei einer solchen Überwachung auch der Inhalt von E-Mails und damit personenbezogene Informationen des Senders und des Empfängers der E-Mail untersucht werden, die nicht unbedingt mit dem gleichen Internetdienstanbieter eine vertragliche Beziehung unterhalten. In diesen Fällen würde der Internetdiensteanbieter nämlich personenbezogene Daten (Name, E-Mail-Adresse und möglicherweise sensible Inhaltsdaten) von Nicht-Kunden verarbeiten. Aus praktischer Sicht mag es schwieriger sein, die Einwilligung solcher Personen einzuholen, da dies eher fallweise und weniger beim Abschluss eines Vertrags über einen Telekommunikationsdienst geschehen sollte. Auch kann man realistischerweise nicht davon ausgehen, dass die Einwilligung des Abonnenten auch im Namen anderer gegeben wurde, wie dies häufig in Privathaushalten der Fall ist.

66. In diesem Zusammenhang sollte sich der Internetdiensteanbieter nach Auffassung des EDSB an die bestehenden gesetzlichen Anforderungen halten und Maßnahmen durchführen, die ohne die Überwachung und Untersuchung von Informationen auskommen. Dies ist vor allem von wesentlicher Bedeutung für Kommunikationsdienste, an denen Dritte beteiligt sind, die ihre Einwilligung zur Überwachung nicht geben können; dies gilt insbesondere für versandte und empfangene E-Mails (dies gilt nicht, wenn der Zweck auf Sicherheitserwägungen beruht).

67. Es sei bei dieser Gelegenheit darauf hingewiesen, dass die nationalen Gesetze zur Umsetzung von Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation in diesem Punkt vielleicht nicht immer zufriedenstellend sind, und dass in diesem Zusammenhang generell ein Bedarf an besseren Leitlinien zu den Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation besteht. Der EDSB fordert die Kommission daher auf, hier aktiver zu werden und eine Initiative zu ergreifen, in die Beiträge der in der Artikel 29-Datenschutzgruppe zusammenkommenden Aufsichtsbehörden sowie anderer Akteure einfließen könnten. Bei Bedarf sollte ein Fall vor den Gerichtshof gebracht werden, damit endgültige Klarheit bezüglich der Bedeutung und der Folgen von Artikel 5 Absatz 1 geschaffen wird.

([33]) Unbeschadet der Fälle, in denen im Web-Verkehr personenbezogene Informationen übermittelt werden, wie z. B. Bilder identifizierbarer natürlicher Personen, die auf eine Website gestellt werden. Für die Verarbeitung solcher Daten ist eine Rechtsgrundlage erforderlich, doch fällt sie nicht unter Artikel 5 Absatz 1, da diese Personen keine „betroffenen Nutzer" sind.

V.3 **Verhältnismäßigkeit — Grundsatz der Datenminimierung**

68. In Artikel 6 Buchstabe c der Datenschutzrichtlinie wird der Grundsatz der Verhältnismäßigkeit etabliert ([34]), der auch für Internetdienstanbieter gilt, da sie für die Verarbeitung Verantwortliche im Sinne dieser Richtlinie sind, wenn sie Überwachungs- und Filtermaßnahmen durchführen.

69. Nach diesem Grundsatz dürfen personenbezogene Daten verarbeitet werden, sofern sie „den Zwecken entsprechen, für die sie erhoben oder weiter verarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen". Bei Anwendung dieses Grundsatzes ist die Frage zu prüfen, ob die für die Datenverarbeitung eingesetzten Mittel und die Art der verwendeten personenbezogenen Daten angemessen sind und ob es hinreichend wahrscheinlich ist, dass sie zum Erreichen der Ziele beitragen. Lautet die Antwort, dass mehr Daten erhoben werden, als benötigt werden, ist der Grundsatz nicht gewahrt.

70. Der Frage, ob bestimmte Untersuchungstechniken dem Grundsatz der Verhältnismäßigkeit entsprechen, ist von Fall zu Fall zu prüfen. Abstrakt lassen sich hier keine Schlüsse ziehen. Es lassen sich jedoch verschiedene konkrete Aspekte anführen, die bei der Prüfung der Einhaltung des Grundsatzes der Verhältnismäßigkeit zu betrachten wären.

71. *Menge der verarbeiteten Informationen.* Eine möglichst tief gehende Überwachung des Datenverkehrs von Kunden von Internetdiensteanbietern dürfte in den meisten Fällen übertrieben und ungesetzlich sein. Die Tatsache, dass diese Überwachung mit Mitteln geschieht, die für die betroffenen Personen nicht erkennbar sind, und dass es für sie schwierig sein kann, die Vorgänge zu begreifen, verstärkt noch die Auswirkungen auf ihre Privatsphäre. Internetdienstanbieter sollten überlegen, ob ihnen nicht weniger in die Privatsphäre eindringende Mittel zur Verfügung stehen, mit denen sich das gewünschte Ziel erreichen lässt. Kann beispielsweise die Überwachung von IP Headern statt des Einsatzes von Deep Packet Inspection das gewünschte Ergebnis bringen? Selbst beim Einsatz von Deep Packet Inspection kann vielleicht die Identifizierung nur bestimmter Protokolle die erforderlichen Informationen liefern. Von Bedeutung kann auch die Anwendung von Datenschutzgarantien einschließlich der Pseudo-Anonymisierung sein. Als Ergebnis der Prüfung sollte herauskommen, dass die Datenverarbeitung verhältnismäßig ist.

72. *Die Effekte der Verarbeitung (unmittelbar mit dem Zweck verbunden).* Es mag in Fällen an Verhältnismäßigkeit mangeln, in denen Internetdiensteanbieter Datenverkehrssteuerung betreiben und den Zugang zu bestimmten Diensten ausschließen, ohne jedoch den Nutzern einen angemessenen Anteil an dem dadurch entstehenden Nutzen zukommen zu lassen.

73. Es sei nachdrücklich darauf hingewiesen, dass der Grundsatz der Verhältnismäßigkeit auch dann noch gilt, wenn anderen rechtlichen Anforderungen Genüge getan wurde, also auch, wenn ein Internetdienstanbieter beispielsweise von betroffenen Personen die Einwilligung zur Überwachung von Inhalten erhalten hat. Das bedeutet, dass die im Zuge der Überwachung von Inhalten vorgenommene Datenverarbeitung nach wie vor ungesetzlich sein kann, wenn sie gegen den zugrunde liegenden Grundsatz der Verhältnismäßigkeit verstößt.

V.4 **Sicherheit und organisatorische Maßnahmen**

74. Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation fordert Internetdienstanbieter ausdrücklich auf, geeignete technische und organisatorische Maßnahmen ergreifen, um zu gewährleisten, dass i) nur befugtes Personal Zugriff auf personenbezogene Daten hat und dies nur zu gesetzlich vorgesehenen Zwecken, ii) personenbezogene Daten gegen zufällige oder unrechtmäßige Verarbeitung geschützt sind, und iii) ein Sicherheitskonzept bezüglich der Verarbeitung personenbezogener Daten umgesetzt wird. Ferner wird den nationalen zuständigen Behörden die Möglichkeit zur Überprüfung dieser Maßnahmen gegeben.

75. Gemäß Artikel 4 Absatz 3 und 2 der Datenschutzrichtlinie für elektronische Kommunikation sind Internetdienstanbieter ferner verpflichtet, den jeweiligen nationalen zuständigen Behörden Verstöße gegen die Datensicherheit zu melden und die betroffenen Personen zu unterrichten, falls die Weitergabe für sie nachteilige Folgen haben könnte.

76. Die Verarbeitung personenbezogener Daten in Nachrichten mit dem Ziel der Datenverkehrssteuerung kann dem Internetdiensteanbieter Zugriff auf Daten gewähren, die noch sensibler als Verkehrsdaten sind.

([34]) Wie bereits ausgeführt, findet die Datenschutzrichtlinie auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten Anwendung, die in der Datenschutzrichtlinie für elektronische Kommunikation nicht ausdrücklich geregelt sind.

77. Die von den Internetdiensteanbietern ausgearbeiteten Sicherheitsvorkehrungen sollten daher besondere Garantien dafür enthalten, dass die Maßnahmen diesen Risiken angemessen sind. Gleichzeitig sollten die nationalen zuständigen Behörden, die diese Maßnahmen überprüfen, besonders anspruchsvoll sein. Schließlich sollte gewährleistet sein, dass wirksame Meldeverfahren eingeführt werden, mit denen betroffene Personen unterrichtet werden, deren Daten in Gefahr geraten sind und die daher mit nachteiligen Folgen zu rechnen haben.

VI. **VORSCHLÄGE FÜR POLITISCHE UND GESETZGEBERISCHE MASSNAHMEN**

78. Untersuchungstechniken, die auf Verkehrsdaten und der Untersuchung von IP Payloads, also den Inhalten von Nachrichten basieren, können Auskunft über die Internetaktivitäten von Nutzern geben: besuchte Websites und Aktivitäten auf diesen Websites, Nutzung von P2P-Anwendungen, heruntergeladene Dateien, gesendete und empfangene E-Mails, von wem sie stammen, ihr Thema, wie sind sie formuliert, usw. Internetdienstanbieter könnten diese Informationen verwenden wollen, um bestimmte Datenverkehre wie z. B. Video-on-Demand anderen gegenüber vorrangig zu behandeln. Sie könnten sie zur Identifizierung von Viren heranziehen oder auch zur Entwicklung von Profilen für verhaltensorientierte Werbung. Alle diese Vorgehensweisen stellen einen Eingriff in das Recht auf Vertraulichkeit der Kommunikation dar.

79. Je nach den verwendeten Techniken und den Besonderheiten des Falls nehmen die Auswirkungen auf die Privatsphäre zu. Je mehr Daten abgefangen und je tiefer die erhobenen Daten analysiert werden, desto größer ist der Konflikt mit dem Grundsatz der Vertraulichkeit der Kommunikation. Das Ausmaß, in dem ein Eingriff in die Privatsphäre und in den Datenschutz betroffener Personen stattfindet, wird entscheidend auch dadurch bestimmt, zu welchen Zwecken die Überwachung stattfindet und welche Datenschutzgarantien zum Tragen kommen. Das Sperren und Überwachen zwecks Bekämpfung von Malware, mit strengen Auflagen für die Speicherung und Verwendung der untersuchten Daten, kann nicht mit Situationen verglichen werden, in denen die Daten aufgezeichnet werden, um individuelle Profile für verhaltensorientierte Werbung zu erstellen.

80. Grundsätzlich ist der EDSB der Auffassung, dass der bestehende EU-Rahmen für den Schutz der Privatsphäre und den Datenschutz bei korrekter Auslegung, Anwendung und Durchsetzung durchaus gewährleisten könnte, dass das Recht auf Vertraulichkeit gewahrt und dass ganz allgemein der Schutz der Privatsphäre und der Daten betroffener Personen nicht gefährdet wird. ([35]) Internetdienstanbieter sollten solche Mechanismen nur einsetzen, wenn sie den Rechtsrahmen ordnungsgemäß angewandt haben. Zu den wichtigsten einschlägigen Bestandteilen des Rahmens, die Internetdiensteanbieter einhalten sollten, gehören unter anderem folgende:

— Internetdiensteanbieter dürfen gemäß den Artikeln 4 und 6 der Datenschutzrichtlinie für elektronische Kommunikation Datenverkehrssteuerung mit der Absicht betreiben, die Sicherheit des Dienstes zu gewährleisten, den Dienst bereitzustellen sowie Überlastungen des Netzes zu beschränken.

— Wenn Internetdiensteanbieter eine Datenverkehrssteuerung zu anderen als den vorstehend genannten Zwecken betreiben möchten, die die Verarbeitung von Verkehrs- und/oder Kommunikationsdaten zur Folge hat, benötigen sie eine weitere spezifische Rechtsgrundlage und möglicherweise die Einwilligung der Nutzer. So ist zum Beispiel die in Kenntnis der Sachlage gegebene Einwilligung der Nutzer erforderlich, um den Datenverkehr betroffener Personen zum Zweck der Einschränkung (oder Zulassung) des Zugangs zu bestimmten Anwendungen und Diensten wie P2P oder VoIP zu überwachen und zu filtern.

— Die Einwilligung muss ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben werden. Sie sollte durch aktives Handeln der Nutzer erfolgen. Mit diesen Anforderungen wird nachdrücklich unterstrichen, dass verstärkt für eine angemessene Information der betroffenen Personen zu sorgen ist; diese Informationen müssen direkt gegeben werden, verständlich und spezifisch sein, damit die Personen die Wirkungen der Verfahren beurteilen und letztendlich eine Entscheidung in Kenntnis der Sachlage treffen können. In Anbetracht der Komplexität dieser Techniken ist die Vermittlung aussagekräftiger Vorabinformationen eine der Hauptvoraussetzungen für eine gültige Einwilligung. Am Rande sei noch erwähnt, dass den Nutzern, die einer Überwachung nicht zustimmen, keine nachteiligen Folgen (einschließlich Kosten) entstehen dürfen.

([35]) Dies gilt unbeschadet der notwendigen Rechtsänderungen aufgrund anderer Erwägungen, insbesondere vor dem Hintergrund der allgemeinen Überarbeitung des EU-Rechtsrahmens für den Datenschutz, der mit Blick auf neue Technologien und die Globalisierung wirksamer gestaltet werden soll.

— Unabhängig von der Rechtsgrundlage der Verarbeitung und ihrem Zweck spielt der Grundsatz der Verhältnismäßigkeit eine zentrale Rolle, sobald ein Internetdiensteanbieter Datenverkehrssteuerung betreibt: Bereitstellung des Dienstes, Vermeidung von Überlastung oder Anbieten gezielter Abonnements mit oder ohne Zugang zu bestimmten Diensten und Anwendungen. Dieser Grundsatz schränkt die Internetdiensteanbieter in ihren Möglichkeiten ein, eine Überwachung der Inhalte von Nachrichten vorzunehmen, die die Verarbeitung erheblicher Datenmengen zur Folge hat oder allein für die Internetdiensteanbieter von Nutzen ist. Was Internetdiensteanbieter logistisch bewältigen können, hängt davon ab, wie weit die Techniken in die Privatsphäre eindringen, welche Ergebnisse gewünscht werden (die ihnen unter Umständen Nutzen bringen), und welche besonderen Garantien für den Schutz der Privatsphäre und den Datenschutz angewandt werden. Vor dem Einsatz von Untersuchungstechniken müssen Internetdiensteanbieter prüfen, ob diese dem Grundsatz der Verhältnismäßigkeit entsprechen.

81. Derzeit enthält der Rechtsrahmen zwar einschlägige Bedingungen und Garantien, doch sollte besonders darauf geachtet werden, ob Internetdiensteanbieter den gesetzlichen Anforderungen tatsächlich entsprechen, ob sie die Verbraucher mit den erforderlichen Informationen versorgen, damit diese sinnvolle Entscheidungen treffen können, und ob sie den Grundsatz der Verhältnismäßigkeit wahren. Auf nationaler Ebene umfassen die für das vorstehend Ausgeführte zuständigen Behörden zum einem die Telekommunikationsbehörden und zum anderen die Datenschutzbehörden. Auf EU-Ebene gehört zu den einschlägigen EU-Stellen auch das GEREK. Aber auch der EDSB könnte in diesem Zusammenhang eine Rolle spielen.

82. Über die Überwachung der derzeitigen Einhaltung der Vorschriften hinaus und in Anbetracht der relativ neuartigen Möglichkeit, Datenverkehr massiv und in Echtzeit zu untersuchen, bedürfen einige Aspekte der in dieser Stellungnahme diskutierten Anwendung des Rahmens einer gründlicheren Analyse und weiterer Klarstellung. So sind Leitlinien unter anderem zu folgenden Bereichen besonders wichtig:

— Bestimmung rechtmäßiger Untersuchungstechniken, um einen reibungslosen Fluss des Datenverkehrs zu gewährleisten, die möglicherweise keine Einwilligung der Nutzer erfordern, wie beispielsweise die Bekämpfung von Spam. Neben der Frage, wie weit die Überwachung in die Privatsphäre eindringt, sind Aspekte wie beispielsweise das Ausmaß an Störungen des reibungslosen Verkehrsflusses, die andernfalls aufträten, von Bedeutung;

— Bestimmung der Untersuchungstechniken, die zu Sicherheitszwecken angewandt werden können und keine Einwilligung der Nutzer erfordern;

— Bestimmung der Umstände, unter denen die Einwilligung der betroffenen Personen erforderlich ist, insbesondere die Einwilligung aller betroffenen Nutzer, sowie der zulässigen technischen Parameter, um zu gewährleisten, dass die technische Untersuchung keine Datenverarbeitung zur Folge hat, die in keinem Verhältnis zu den angestrebten Zwecken steht;

— in den drei vorstehend genannten Fällen könnten auch Hinweise zur Anwendung der erforderlichen Datenschutzgarantien (Zweckbindung, Sicherheit usw.) erforderlich sein.

83. In Anbetracht der Tatsache, dass die Zuständigkeiten in diesem Bereich sowohl auf nationaler wie auf EU-Ebene liegen, ist der EDSB der Ansicht, dass einem Austausch von Meinungen und Erfahrungen auf der Suche nach harmonisierten Vorgehensweisen zentrale Bedeutung zukommt. Zu diesem Zweck schlägt der EDSB die Schaffung einer Plattform oder einer Expertengruppe vor, in der sich Vertreter der nationalen Regulierungsbehörden, die Artikel 29-Datenschutzgruppe, der EDSB und das GEREK treffen. Erstes Ziel dieser Plattform wäre die Ausarbeitung eines Leitfadens, zumindest zu den oben genannten Punkten, damit fundierte und harmonisierte Konzepte und gleiche Voraussetzungen für alle geschaffen werden. Der EDSB fordert die Kommission auf, diese Initiative ins Leben zu rufen.

84. Zu guter Letzt müssen sowohl die nationalen Behörden als auch die entsprechenden EU-Stellen einschließlich GEREK und Europäische Kommission sorgfältig die Marktentwicklungen in diesem Bereich beobachten. Aus dem Blickwinkel des Datenschutzes und des Schutzes der Privatsphäre wäre ein Szenario höchst problematisch, in dem Internetdiensteanbieter routinemäßig Datenverkehrssteuerung betreiben und Abonnements anbieten, die sich auf einen gefilterten Zugang zu Inhalten und Anwendungen stützen. Sollte dieser Fall jemals eintreten, müssten Gesetze zur Regelung dieser Situation erlassen werden.

VII. **SCHLUSSFOLGERUNGEN**

85. Die Tatsache, dass Internetdiensteanbieter zunehmend auf Überwachung und Untersuchungstechniken setzen, wirkt sich auf die Neutralität des Internets und die Vertraulichkeit der Kommunikation aus. Dabei entstehen ernstzunehmende Probleme für den Schutz der Privatsphäre und der personenbezogenen Daten der Nutzer.

86. In der Mitteilung der Kommission „Offenes Internet und Netzneutralität in Europa" werden diese Fragen zwar gestreift, doch meint der EDSB, dass noch mehr zu unternehmen ist, um zu einer zufriedenstellenden zukunftsweisenden Politik zu kommen. In der vorliegenden Stellungnahme hat er daher einen Beitrag zur derzeit stattfindenden Debatte über Netzneutralität und hier vor allem zu den Aspekten Datenschutz und Schutz der Privatsphäre vorgelegt.

87. Nach Auffassung des EDSB sollten die nationalen Behörden und das GEREK die Marktsituation im Auge behalten. Dies sollte zu einem klaren Bild führen, aus dem hervorgeht, ob sich der Markt in Richtung massiver, in Echtzeit erfolgender Untersuchung des Datenverkehrs entwickelt und ob es Probleme bei der Einhaltung des Rechtsrahmens gibt.

88. Die Marktüberwachung sollte einhergehen mit einer weiteren Analyse der Wirkungen neuer Vorgehensweisen auf den Datenschutz und den Schutz der Privatsphäre im Internet. In der vorliegenden Stellungnahme werden einige Bereiche genannt, in denen Klarstellungen erforderlich sind. Zwar sind EU-Agenturen und Einrichtungen wie das GEREK, die Artikel 29-Datenschutzgruppe und der EDSB durchaus in der Lage, die Bedingungen für die Anwendung des Rahmens klarzustellen, doch meint der EDSB, dass es Pflicht der Kommission wäre, die Debatte zu koordinieren und zu lenken. Daher fordert er die Kommission auf, mit diesem Ziel eine Initiative in Form einer Plattform oder Arbeitsgruppe ins Leben zu rufen, an der alle genannten Akteure mitwirken. Unter anderem folgende Bereiche bedürfen weiterer Analysen:

— Bestimmung der rechtmäßigen Untersuchungstechniken, mit denen ein reibungsloser Datenfluss gewährleistet werden kann, und die zu Sicherheitszwecken angewandt werden können;

— Bestimmung der Umstände, unter denen die Einwilligung der betroffenen Personen erforderlich ist, insbesondere die Einwilligung aller betroffenen Nutzer, sowie der zulässigen technischen Parameter, um zu gewährleisten, dass die technische Untersuchung keine Datenverarbeitung zur Folge hat, die in keinem Verhältnis zu den angestrebten Zwecken steht;

— in den vorstehend genannten Fällen könnten auch Hinweise zur Anwendung der erforderlichen Datenschutzgarantien (Zweckbindung, Sicherheit usw.) erforderlich sein.

89. Je nach den Ergebnissen könnten weitere gesetzgeberische Maßnahmen erforderlich sein. In diesem Fall sollte die Kommission politische Maßnahmen vorschlagen, mit denen der Rechtsrahmen gestärkt und die Rechtssicherheit gewährleistet wird. In neuen Maßnahmen sollten die praktischen Konsequenzen des Grundsatzes der Netzneutralität klar umrissen werden, wie dies bereits in einigen Mitgliedstaaten geschehen ist, und sie sollten dafür sorgen, dass die Nutzer eine echte Wahlmöglichkeit haben, indem vor allem die Internetdiensteanbieter gezwungen werden, unüberwachte Verbindungen anzubieten.

Brüssel, den 7. Oktober 2011

Peter HUSTINX

Europäischer Datenschutzbeauftragter