KOMMENTARE DES EDSB ZUR ÖFFENTLICHEN KONSULTATION DER GD CONNECT *"SPECIFIC ASPECTS OF TRANSPARENCY, TRAFFIC MANAGEMENT AND SWITCHING IN AN OPEN INTERNET"* (SPEZIFISCHE FRAGEN DER TRANSPARENZ, DER VERKEHRSSTEUERUNG UND DES ANBIETERWECHSELS IN EINEM OFFENEN INTERNET)

Die Europäische Kommission hat eine öffentliche Konsultation eingeleitet, die darauf abzielt, Stellungnahmen zu spezifischen Aspekten einzuholen, die sich als Schlüsselfragen der seit einigen Jahren in Europa geführten Debatte über die Netzneutralität herauskristallisiert haben. Ein vorrangiges Anliegen des Vorgehens der Kommission in diesem Zusammenhang ist es, den Verbraucher durch politische Maßnahmen in den Bereichen der Transparenz, des Anbieterwechsels und bestimmter Aspekte der Datenverkehrssteuerung, einschließlich der "Deep-Packet-Inspection"-Technologien (DPI), in die Lage zu versetzen, auf einem wettbewerbsorientierten Markt mit klaren Regeln eine gut informiert Wahl zu treffen.[1]

Der EDSB begrüßt die Initiative der Kommission, zu Fragen bezüglich der Netzneutralität eine breite Konsultation interessierter Kreise unter Einbeziehung des privaten und des öffentlichen Sektors sowie Gruppen der Zivilgesellschaft durchzuführen. Der EDSB betrachtet diese Konsultation als einen wichtigen Teil der Debatte, die stattfinden muss, bevor politische Empfehlungen oder Rechtsvorschriften ausgearbeitet werden.

Der EDSB nimmt zur Kenntnis, dass die Initiative der Kommission auf einer Untersuchung zur Verkehrssteuerung basiert, die vom Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK)[2] auf Ersuchen der Kommission durchgeführt wurde.

I. Relevanz des Schutzes personenbezogener Daten im Kontext der Debatte zur Netzneutralität

Verkehrssteuerungspraktiken, insbesondere solche, die eine Prüfung der Kommunikation der Bürger im Internet mithilfe von DPI-Technologien umfassen, bergen große Risiken für den Schutz der Privatsphäre und der personenbezogenen Daten natürlicher Personen. Durch eine Prüfung der Kommunikationsdaten können Internetdienstanbieter in das Recht auf Privatsphäre natürlicher Personen eingreifen und die Vertraulichkeit der Kommunikation verletzen, beides Grundrechte, die in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) und Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (die „Charta") verankert sind und in die

[1] Mithilfe von DPI-Technologien werden verschiedene Schichten von Datenpaketen überprüft ("Header"- und Inhaltsteil) und die Pakete je nach Ergebnis weiterverarbeitet. Zu den daraus resultierenden Maßnahmen zählen das "Routing", die Priorisierung, das Sperren von Paketen, *etc.*, je nach den vorab definierten Richtlinien. Beispiele von daraus resultierenden Maßnahmen sind die Priorisierung oder das Filtern des "VoIP"- oder "P2P"-Verkehrs durch Internetdienstanbieter oder sicherheitsspezifische Maßnahmen, falls "Malware" in den Paketen festgestellt wird.

[2] Vgl. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf .

Postanschrift: Rue Wiertz – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

Datenschutzrichtlinie 95/46/EG und verbundene Rechtsinstrumente aufgenommen wurden. Die Vertraulichkeit ist auch im EU-Sekundärrecht geschützt, insbesondere in Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation[3].

Die Bedeutung des Schutzes der Privatsphäre und des Datenschutzes wächst mit der Konvergenz der gesamten Kommunikation im Internet und der immer zentraleren Rolle, die das Internet im Leben aller einnimmt. Internetdienstanbieter könnten beispiellose Einblicke in das Privatleben ihrer Benutzer erlangen, falls sie freien Zugang zu deren Kommunikation hätten und diese zu eigenen Zwecken verarbeiten könnten.

Der EDSB hat bereits mehrfach zur Debatte beigetragen, insbesondere im Rahmen der Kommentare zur öffentlichen Konsultation der Kommission „Offenes Internet und Netzneutralität“[4] und der Stellungnahme des EDSB über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten.[5]

Dennoch möchten er anlässlich der öffentlichen Konsultation bestimmte Aspekte unterstreichen, die darin aufgeworfen werden, damit die Kommission die Kommentare des EDSB bei der Ausarbeitung zukünftiger politischer Aktionen in diesem Bereich berücksichtigen kann.

II. Allgemeine Frage: Internetverkehrssteuerung und personenbezogene Daten (Frage 9)

Wie in seiner Stellungnahme zur Netzneutralität bereits ausgeführt, unterstützt der EDSB ein offenes Internet. Die Internetdienstanbieter sind befugt, Verkehrssteuerungsmaßnahmen zu entwickeln, vorausgesetzt diese garantieren die volle Einhaltung der Anforderungen an den Schutz der Privatsphäre und den Datenschutz.

Der Einsatz von DPI-Technologien macht es erforderlich, dass die Internetdienstanbieter beachtliche Datenmengen im Zusammenhang mit Internetnutzern verarbeiten, wobei viele dieser Daten als personenbezogen (z. B. IP-Adressen), vertraulich (z. B. der Inhalt der Kommunikation)[6] oder sogar sensibel (z. B. Daten über die Gesundheit) betrachtet werden. Gemäß Artikel 7 der Datenschutzrichtlinie 95/46/EG und Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation muss eine angemessene Rechtsgrundlage gefunden werden, um die Verarbeitung personenbezogener Daten im Kontext der Internetverkehrssteuerung zu rechtfertigen.

---

[3] 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, in der Fassung der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009.

[4] Kommentare des EDSB zur öffentlichen Konsultation der Kommission zum Thema „Offenes Internet und Netzneutralität in Europa“, 6. Oktober 2010, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_DE.pdf.

[5] Siehe Stellungnahme des EDSB über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten, 7. Oktober 2011, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_DE.pdf.

[6] Siehe Stellungnahme der Artikel-29-Datenschutzgruppe zum Begriff „personenbezogene Daten“, 20. Juni 2007, S.16-17, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.

Die Verkehrssteuerung wird von den Internetdienstanbietern zu vielen unterschiedlichen Zwecken durchgeführt. Zu den traditionellen Zwecken zählen die Netzsicherheit und das Engpassmanagement. Die Techniken zur Prüfung des Datenverkehrs basieren auf der Analyse der Internetprotokolle auf unterschiedlichen Schichten des Datenpakets, hauptsächlich zum Einlesen der Quell- und Ziel-IP-Adressen und der Internetprotokolle, was in den meisten Fällen zu Zwecken des Engpassmanagements und der Verkehrsbeschränkung ausreichend ist. Wie der EDSB bereits im Detail in seiner Stellungnahme zur Netzneutralität[7] ausgeführt hat, dürfen die Internetdienstanbieter gemäß der Datenschutzrichtlinie für elektronische Kommunikation diese Art der Verarbeitung zu Zwecken der Übertragung von Mitteilungen in der Regel durchführen, um die Sicherheit des Kommunikationsdienstes zu gewährleisten oder Engpässe zu reduzieren.

Im Laufe der Jahre sind neue Zwecke hinzugekommen, wie die Leistungsspezialisierung und die Differenzierung des Niveaus der Dienstleistung, eventuell ausgehend von Verträgen mit Kunden, welche zu einer Prüfung und einem Filtern des Internetverkehrs, je nach spezifischer Leistung/Anwendung, führen. Zu den neueren Zielsetzungen, welche eine umfassende Prüfung des Internetverkehrs mit sich bringen, zählen die Verhaltensanalyse und das "Profiling", die hauptsächlich zu Sicherheitszwecken, aber auch zu kommerziellen Zwecken, zum Schutz der Urheberrechte und zu anderen Zwecken durchgeführt werden. Diese neue Zwecke sind vom Standpunkt des Schutzes der Privatsphäre und des Datenschutzes weitaus einschneidender als die traditionellen Zwecke, insbesondere sofern diese eine Überwachung des Online-Verhaltens der Internetnutzer zur Folge haben[8]. Wie der EDSB in seiner Stellungnahme zur Netzneutralität bereits ausgeführt hat[9], könnten einige der Verarbeitungen über das hinausgehen, was rechtlich zulässig wäre. Insbesondere wenn diese Verarbeitungen nicht explizit im Rahmen der Datenschutzrichtlinie für elektronische Kommunikation vorgesehen sind und/oder nicht voll mit den anderen Pflichten der Internetdienstanbieter vereinbar sind, wie denjenigen gemäß Artikel 15 der Richtlinie über den elektronischen Geschäftsverkehr, muss eingehend geprüft werden, ob zumindest (i) jede dieser Verarbeitungen erforderlich und angesichts des verfolgten Ziels angemessen ist und (ii) ob eine ausreichende Gesetzesgrundlage gemäß Artikel 7 der Richtlinie 95/46/EG gegeben ist. In Ermangelung einer rechtlichen Grundlage sollten diese auf einer anderen Rechtsgrundlage, wie Konsens, basieren.

Folglich sollten Maßnahmen im Bereich der Verkehrssteuerung unter voller Achtung der Grundrechte und in Übereinstimmung mit dem bestehenden Rechtsrahmen für die elektronische Kommunikation, den elektronischen Geschäftsverkehr und den Datenschutz ausgearbeitet werden.

III. Besondere Kommentare

a) DPI-Technologien und Risiken für den Schutz der Privatsphäre (Frage 10a)

[7] Vgl. weitere Einzelheiten in der Stellungnahme des EDSB zur Netzneutralität, Seiten 10-12.

[8] Maßnahmen, die auf eine allgemeine Überwachung des Internets abzielen, können nur nach Maßgabe der Rechtsvorschriften durchgeführt werden (insbesondere Artikel 15 der Richtlinie über den elektronischen Geschäftsverkehr). Dieser Grundsatz wurde vom Europäischen Gerichtshof in der Rechtssache C-70/10, Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) in Erinnerung gerufen, Urteil vom 24. November 2011.

[9] Siehe Stellungnahme des EDSB, Seiten 10-14.

Eine detaillierte Beschreibung der durch den Einsatz der DPI-Technologien aufgeworfenen Fragen im Zusammenhang mit dem Schutz der Privatsphäre und dem Schutz personenbezogener Daten ist in der Stellungnahme des EDSB zur Netzneutralität enthalten[10]. Die Risiken für den Schutz der Privatsphäre, den Datenschutz und die Vertraulichkeit der Kommunikation sind sehr hoch, aufgrund der stark eingreifenden Merkmale der DPI-Technologien, mit denen der gesamte Inhalt von IP-Paketen geprüft wird, um, ausgehend von vordefinierten Kriterien, die im Rahmen von Prüfrichtlinien festgelegt werden, spezifische Muster ausfindig zu machen.

Aufgrund der wachsenden Konvergenz aller Kommunikationsarten im Internet, einschließlich derjenigen, die sensible personenbezogene Daten enthalten, sind die Auswirkungen dieser Maßnahmen noch stärker. Außerdem verlagert sich inzwischen auch die traditionelle Kommunikation immer stärker in das Internet. Der allgegenwärtige Zugang wird verstärkt durch das wachsende Serviceangebot für „intelligente“ mobile Endgeräte. Außer den Standortdaten, die mit traditionellen Telefonzellen verbunden sind, die zu den gewöhnlich verarbeiteten Daten hinzukommen, gestattet es die Verwendung „intelligenter“ Endgeräte über Sensoren, die in diesen Geräten eingebaut sind, weitere Informationen einzuholen, wie feinmaschige Standortdaten dank GPS-Antennen und hochauflösenden Kameras. In einigen Fällen (Verwendung derselben Internetdienstanbieter und sogar desselben Gateways) werden ganz unterschiedliche Arten von Kommunikationsflüssen über denselben Zugangspunkt übermittelt, wodurch die physikalische Konvergenz personenbezogener Daten im Zusammenhang mit derselben Person und den anderen Personen, mit denen diese kommuniziert, erhöht wird.

Als Folge davon könnten Internetdienstanbieter größere Datenmengen bezüglich einer Person erfassen, welche eine umfassende Nachrichtengewinnung und ein "Profiling" erleichtern. Außerdem könnte die Versuchung bestehen, unrechtmäßig zusammengetragene personenbezogene Daten zu kommerziellen Zwecken zu verwenden, insbesondere für verhaltensbasierte und zielgerichtete Werbung. Die Erfahrung hat gelehrt, dass die Verfügbarkeit neuer Datenerfassungs- und Verarbeitungsmöglichkeiten oft Interesse an der Verwendung der verfügbaren Daten zu neuen Zwecken weckt, die über das hinausgehen, was ursprünglich beabsichtigt war und den betroffenen Personen mitgeteilt und mit diesen vereinbart wurde. Die Einrichtung umfassender Infrastrukturen für DPI-Technologien in Kommunikationsnetzwerken kann zu einem derartigen Interesse führen, z. B. aus wirtschaftlichen Gründen oder aus Gründen der Strafverfolgung. Sofern diese Infrastruktur nicht mit Mitteln ausgestattet ist, um unzulässige Nutzung aufzudecken, kann es schwierig sein, Verletzungen des Schutzes der Privatsphäre aufzuspüren und nachzuweisen.

b) Verkehrssteuerung und Alternativen zu DPI-Technologien (Frage 10b)

Bei traditionellen Verkehrssteuerungstechniken werden die Informationsfelder des "Header"-teils des Datenpakets verwendet, um Datenpaketflüsse zu verarbeiten. Einige der neuen Internetapplikations-/Servicearten können nicht mehr identifiziert werden, indem lediglich die Protokollfelder geprüft werden, sondern enthalten die Identität in den "Payload"-Daten der Pakete[11]. Teilweise geschieht dies absichtlich (Änderung des Standard-TCP/UDP-Ports, "Tunneling", *etc.*), um eine einfache Identifizierung der Applikation zu vermeiden. Zu

[10] Siehe Abschnitt V.4, S. 17.

[11] Im Hinblick auf eine grundlegende Einführung zur Übermittlung von Informationen über das Internet und Prüftechniken wird verwiesen auf die Absätze IV.1 und IV.2 der Stellungnahme, *op. cit.*

Zwecken einer feinmaschigeren Kontrolle werden die Informationen in den "Payload"-Daten gesucht.

Der EDSB glaubt, dass die Suche nach Alternativen zu DPI-Technologien, bei denen ein größerer Schutz der Privatsphäre gewährleistet wird, unterstützt werden sollte. In diesem Zusammenhang sei auf die folgenden spezifischen Punkte hingewiesen, die berücksichtigt werden sollten, um zur Entwicklung von Alternativen beizutragen, bei denen der Schutz der Privatsphäre stärker gewährleistet ist:

- Die Grundsätze der Zweckbindung und der Angemessenheit sollten stets als Anhaltspunkte betrachtet werden bei der Prüfung und Umsetzung aktueller und zukünftiger Verkehrs- und Kommunikationssteuerungs- bzw. Verarbeitungstechniken. Gemäß dem in Artikel 6 Absatz c der Richtlinie 95/46/EG verankerten Grundsatz der Angemessenheit darf die Verarbeitung personenbezogener Daten nicht über die Zwecke hinausgehen, für die sie erhoben werden. Wie der EDSB in seiner Stellungnahme festgestellt hat, sollte der Grundsatz der Angemessenheit den Internetdienstanbietern als Leitprinzip dienen; dieses Leitprinzip sollte den Einsatz weniger eingreifender Methoden zur Prüfung elektronischer Kommunikation und die Anwendung von Datenschutzgarantien fördern, wie beispielsweise einer *Pseudoanonymisierung*.[12]

- Das Verfahren zur Standardisierung von Kommunikationsprotokollen hat stets darauf abgezielt, die Applikations-/Service-Informationsfelder auf der Protokollebene festzusetzen (generell per Definition auf der Applikationsebene). Der EDSB glaubt, dass diese grundsätzliche Absicht in der Zukunft beibehalten werden sollte und unterstützt Anstrengungen in Richtung einer Bewertung der aktuellen Angemessenheit des Internet-Protokollstapels im Hinblick auf die aktuellen Marktanforderungen.

- In vielen Fällen können Dienste, welche spezifische Verkehrssteuerungspraktiken erforderlich machen, über die IP-Adressen identifiziert werden, die diese verwenden (z. B. Suchmaschinen, Video-Portale). Die Verwendung der IP-Adresse der angeforderten Dienste als ein Indikator der Art des Dienstes sollte zur Identifizierung des Dienstes verwendet werden. Diese Information könnte auch hilfreich sein für ein besseres "Routing" der angeforderten Ressourcen zum Kunden.

- Studien bezüglich der Methoden, welche ein Ableiten der angeforderten Service-/Applikationsart ausgehend von einigen statistischen Merkmalen der Pakete und der Paketflüsse möglich machen, sollten gefördert werden.

- Ein angemessenes Angebot mit einer Bandbreite, bei der berücksichtigt wird, was im Vertrag zwischen dem Internetdienstanbieter und den Abonnenten definiert ist, würde das Problem einschränken.

c) Prüfung der Kommunikation, Sicherheit und Maßnahmen im Rahmen der Rechenschaftspflicht

[12] Siehe EDSB über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten, 7. Oktober 2011, Absätze 68-72, *op.cit.*

Wie der EDSB in seiner Stellungnahme[13] erläutert hat, sieht Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation explizit vor, dass die Internetdienstanbieter technische und organisatorische Maßnahmen ergreifen, die ein *Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.*[14]

Angesichts der Tatsache, dass – wie oben in Abschnitt I.a) beschrieben – das Scannen der "Payload" von Paketen eine aufgrund der möglichen Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz mit hohen Risiken verbundene Verarbeitung darstellt, müssen die technischen und organisatorischen Maßnahmen zu deren Schutz ebenfalls weitgehend und effektiv genug sein, um diesen Risiken entgegenzuwirken, insbesondere im Hinblick auf den möglichen Missbrauch der Daten.

Die in Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation als verbindlich vorgeschriebene Umsetzung eines „Sicherheitskonzept[s] bezüglich der Verarbeitung personenbezogener Daten" sollte das Ergebnis einer angemessenen Bewertung der Risiken für die Grundfreiheiten sein. Es sei angemerkt, dass der Vorschlag der Kommission für eine Datenschutz-Grundverordnung (nachfolgend: „der Verordnungsvorschlag"[15]), explizit eine „Risikobewertung"[16] vorsieht, um die zweckmäßigsten Maßnahmen zu bestimmen. Artikel 33 des Verordnungsvorschlags sieht bei bestimmten Verarbeitungsvorgängen, die konkrete Risiken für den Schutz der Privatsphäre und den Datenschutz bergen, eine Datenschutz-Folgeabschätzung vor. In diesem Zusammenhang unterstützt der EDSB eine weitere Bewertung derjenigen DPI-Praktiken, welche eine Datenschutz-Folgeabschätzung zwingend erforderlich machen.

Die Wahrung der Privatsphäre durch Technik und datenschutzfreundliche Voreinstellungen (gemäß Artikel 23 des Verordnungsvorschlags) sollte von den Internetdienstanbietern bei der Einrichtung ihrer Infrastruktur und der Dienstleistungen berücksichtigt werden. Die Wahrung der Privatsphäre durch Technik und datenschutzfreundliche Voreinstellungen hat Auswirkungen auf das Leistungsangebot an die Abonnenten. So sollten die Internetdienstanbieter beispielsweise Dienste anbieten, bei denen die Verarbeitung/das Filtern personenbezogener Daten möglichst beschränkt ist. Die Grundsätze der Wahrung der Privatsphäre durch Technik und datenschutzfreundliche Voreinstellungen sollten auch von Unternehmen berücksichtigt werden, die Lösungen für das allgemeine und spezialisierte Verkehrsmanagement anbieten.

---

[13] Siehe Abschnitt V.4, S.17, *op.cit.*

[14] Diese Maßnahmen gewährleisten zumindest, 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 und Empfehlungen über bewährte Verfahren bezüglich des Sicherheitsniveaus auszugeben, die diese Maßnahmen erzielen sollen. Im Falle einer Datenverletzung muss der Interndienstanbieter die nationale Datenschutzbehörde informieren. Sind personenbezogene Daten oder der Schutz der Privatsphäre der Abonnenten betroffen, sind die Internetdienstanbieter verpflichtet, diese unverzüglich über den Zwischenfall zu informieren, es sei denn, sie sind in der Lage, den Nachweis dafür zu erbringen, dass sie Maßnahmen ergriffen haben, um die Vertraulichkeit dieser Daten zu wahren. Vorbeugend müssen die Internetdienstanbieter die Abonnenten auch über besondere Risiken der Verletzung der Sicherheit des Netzwerks informieren.

[15] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 25. Januar 2012, KOM(2012) 11 endgültig, derzeit Gegenstand des Rechtsetzungsverfahrens durch das Europäische Parlament und den Rat.

[16] Siehe Artikel 30 Absatz 2 des Verordnungsvorschlags.

Außerdem könnte der Rückgriff der Internetdienstanbieter auf sachdienliche Datenschutz-Zertifizierungsprogramme und -siegel das Vertrauen in eine datenschutzfreundliche Verarbeitung stärken und den jeweiligen Markt beflügeln.

Der EDSB glaubt, dass die Internetdienstanbieter ein hohes Maß der Verantwortung (wie in Artikel 22 des Verordnungsvorschlags vorgesehen) nicht nur gegenüber den zuständigen Behörden sondern auch gegenüber den betroffenen Personen an den Tag legen sollten.

Abschließend werden die betroffenen nationalen Behörden, z. B. die Datenschutzbehörden, in der Lage sein, die Sicherheitsmaßnahmen zu überprüfen, wie in Artikel 4 der Datenschutzrichtlinie für die elektronische Kommunikation vorgesehen.

d) Transparenz und Einwilligung der betroffenen Person zur Verkehrssteuerung (Fragen 10 und 11)

Angesichts der großen Risiken, welche bestimmte Verkehrssteuerungstechniken für betroffene Personen mit sich bringen, hat der EDSB wiederholt Transparenz seitens der Internetdienstanbieter gefordert. Die Abonnenten der Kommunikationsdienste haben Anspruch auf angemessene Informationen bezüglich der Geschäftspraktiken der Internetdienstanbieter. Diese Vorgabe hinsichtlich der Transparenz erstreckt sich in Wirklichkeit auf alle von der Kommunikation betroffenen Benutzer. Die Möglichkeit der Verbraucher, eine gut informierte Wahl zu treffen, hängt von der Transparenz des Dienstanbieters im Hinblick auf seine Geschäftspraktiken ab und ist nur dank dieser Transparenz möglich.

Der EDSB möchte die nachfolgenden Überlegungen bezüglich möglicher Wege einer transparenten Darstellung der Verkehrssteuerungspraktiken ausführen:

- Generell muss der Internetdienstanbieter seinen Kunden angemessene Informationen im Zusammenhang mit den eigenen Verkehrssteuerungspraktiken zur Verfügung stellen. Vom Standpunkt des Datenschutzes aus betrachtet sollten die angemessenen Informationen alle in den Artikeln 10 und 11 der Richtlinie 94/46/EG vorgesehenen Informationen enthalten. Diese Informationen könnten zusammen mit den Vertragsbestimmungen zur Verfügung gestellt werden, sollten jedoch klar sein und sich von den typischen vertraglichen Klauseln abheben.

- Außerdem sollten spezifische Informationen über die Verkehrssteuerungspraktiken zur Verfügung gestellt werden, die eine einschneidendere Verarbeitung zur Folge haben, für welche eine Zustimmung erforderlich ist (wie das Einlesen bestimmter Inhaltsschichten, das "Profiling", *etc.*). Es wäre beispielsweise ratsam, dass der Abonnent in diesen Informationen darauf hingewiesen wird, dass eine derartige Verarbeitung Eingriffe in den Schutz der Privatsphäre und den Datenschutz mit sich bringen kann und es sollte daraus hervorgehen, dass der Abonnent seine Zustimmung jederzeit entziehen kann.

- Zur Einholung einer gültigen Zustimmung zur Anwendung von Verkehrsteuerungspraktiken, welche eine einschneidende Verarbeitung zur Folge haben, müssen die Internetdienstanbieter sicherstellen, dass die Zustimmung auf einer aktiven Bestätigung der betroffenen Person basiert und dass diese ohne Zwang, für den

konkreten Fall und in Kenntnis der Sachlage erteilt wird. Folglich kann die Zustimmung nicht einfach durch Unterschreiben der allgemeinen Vertragsbestimmungen eingeholt werden, da eine derartige Zustimmung nicht als spezifisch genug gewertet werden würde. In diesem Zusammenhang müssen die Internetdienstanbieter sorgfältig feststellen, welche Verarbeitungen eine Zustimmung erforderlich machen und sie müssen sicherstellen, dass sie in der Lage sind, ein zukünftiges "Opt-out" im Hinblick auf diese Verarbeitung einzuhalten.

- Der Internetdienstanbieter trägt die Verantwortung für die Unterrichtung der Kunden bei Aktualisierungen oder Änderungen der eigenen Verkehrssteuerungspraktiken. Ist eine Zustimmung zu derartigen Änderungen oder Aktualisierungen erforderlich, sollten die Internetdienstanbieter wiederum dafür sorgen, dass Abonnenten ihre Wünsche ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage äußern. Die Internetdienstanbieter sollten sich auf die angemessenste Weise an ihre Kunden wenden, um diese über Änderungen zu informieren und deren jeweilige Zustimmung einzuholen, sofern dies erforderlich ist. Eine einfache Bekanntmachung der Änderungen auf der eigenen Website würde keine angemessene Mitteilung derartiger Änderungen darstellen.

Brüssel, den 15. Oktober 2012