EUROPÄISCHES PARLAMENT

2004 *2009*

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

2008/2160(INI)

21.1.2009

ENTWURF EINES BERICHTS

mit einem Vorschlag für eine Empfehlung des Europäischen Parlaments an den Rat
zur Stärkung der Sicherheit und der Grundfreiheiten im Internet
(2008/2160(INI))

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

Berichterstatter: Stavros Lambrinidis

PR_INI_art114

INHALT

Seite

VORSCHLAG FÜR EINE EMPFEHLUNG DES EUROPÄISCHEN PARLAMENTS AN DEN RAT

zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (2008/2160(INI))

Das Europäische Parlament,

– in Kenntnis des Vorschlags für eine Empfehlung an den Rat von Stavros Lambrinidis im Namen der PSE-Fraktion zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (B6-0302/2008),

– unter Hinweis auf den Internationalen Pakt über bürgerliche und politische Rechte, die Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) und die Charta der Grundrechte der Europäischen Union[1], insbesondere die darin enthaltenen Bestimmungen über den Schutz personenbezogener Daten, die freie Meinungsäußerung, die Achtung des Privat- und Familienlebens sowie das Recht auf Freiheit und Sicherheit,

– unter Hinweis auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[2], den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen[3] verarbeitet werden, die Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors[4], den Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen, die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (KOM(2007)0698), die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden[5], und den Schlussantrag des Generalanwalts vom 14. Oktober 2008 in der Rechtssache C-301/06 Irland / Parlament und Rat,

– unter Hinweis auf den Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[6], den Rahmenbeschluss 2001/413/JI des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[7], den Rahmenbeschluss 2008/919/JI des Rates vom

[1] ABl. C 364 vom 18.12.2000, S. 1.
[2] ABl. L 281 vom 23.11.1995, S. 31.
[3] ABl. L 350 vom 30.12.2008, S. 60.
[4] ABl. L 345 vom 31.12.2003, S. 90.
[5] ABl. L 105 vom 13.4.2006, S. 54.
[6] ABl. L 69 vom 16.3.2005, S. 67.
[7] ABl. L 149 vom 2.6.2001, S. 1.

28. November 2008 zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung[1], die Mitteilung der Kommission vom 22. Mai 2007 über „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität“ (KOM(2007)0267), sowie auf die jüngsten Initiativen zur Aufdeckung schwerwiegender Straftaten und des Terrorismus (Projekt „Check the Web“),

– unter Hinweis auf die Arbeiten beim Europarat, bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und bei den Vereinten Nationen sowohl in Bezug auf die Bekämpfung der Kriminalität und der Internetkriminalität als auch in Bezug auf den Schutz der Grundrechte und Grundfreiheiten auch im Internet[2],

– unter Hinweis auf die jüngsten diesbezüglichen Urteile der europäischen Gerichte und der nationalen Verfassungsgerichte, insbesondere das Urteil des Bundesverfassungsgerichts, das ein eigenes Recht auf Schutz der Vertraulichkeit und Integrität der EDV-Systeme[3] anerkennt,

– gestützt auf Artikel 114 Absatz 3 und Artikel 94 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres und der Stellungnahme des Ausschusses für Kultur und Bildung (A6-0000/2009),

A. in der Erwägung, dass die Entwicklung des Internets zeigt, dass es zunehmend zu einem unverzichtbaren Instrument zur Förderung demokratischer Initiativen, einem neuen Forum für politische Debatten (z.B. e-Kampagnen, e-Wahlen), einem wichtigen globalen Instrument für die Wahrnehmung der freien Meinungsäußerung (z.B. Blogs) und für die Entfaltung wirtschaftlicher Tätigkeiten wird;

B. in der Erwägung, dass das Internet der Definition der freien Meinungsäußerung, die in Artikel 11 der Charta der Grundrechte der Europäischen Union verankert ist, zu uneingeschränkter Geltung verhilft, insbesondere, was die Dimension ‚ohne Rücksicht auf Staatsgrenzen’ betrifft;

C. in der Erwägung, dass Transparenz, Achtung der Privatsphäre und ein Umfeld, in dem Vertrauen zwischen den Beteiligten herrscht, für die Schaffung eines nachhaltigen Sicherheitskonzepts im Internet als unerlässlich zu betrachten sind;

D. in der Erwägung, dass das Internet aufgrund der Freiheit, die es bietet, auch als Plattform für Aufrufe zu Gewalt und für undemokratische Botschaften, wie zum Beispiel Anstachelung zu Terroranschlägen, benutzt worden ist, sowie in der Erwägung, dass die Bedrohung durch Cyber-Kriminalität insgesamt weltweit zugenommen hat und Einzelpersonen (auch Kinder) und Netze gefährdet;

---

[1] ABl. L 330 vom 9.12.2008, S. 21.

[2] Bsp.: Übereinkommen des Rates über Cyber-Kriminalität vom 23. November 2001; Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

3 BVerfG, 1 BvR 370/07, 27.2.2008, Absatz-Nr. (1 - 333).
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

E. in der Erwägung, dass effizient und entschieden gegen diese Straftaten vorgegangen werden muss, ohne das sich etwas an dem grundsätzlich freien und offenen Wesen des Internets ändern darf;

F. in der Erwägung, dass es in einer demokratischen Gesellschaft die Bürger sind, die ein Recht darauf haben, täglich die Tätigkeit und die Ansichten ihrer Regierung und von privaten Unternehmen, die Dienstleistungen für sie bereitstellen, zu beobachten und zu beurteilen, und nicht die Regierungen oder Unternehmen, die ein Recht darauf haben, täglich die Tätigkeit und die Ansichten ihrer Bürger zu beobachten und zu beurteilen; in der Erwägung, dass technisch hoch entwickelte Beobachtungsmethoden, zusammen mit laschen Rechtsvorschriften zur Festlegung der Grenzen ihrer Anwendung, diesen Grundsatz zunehmend gefährden;

G. in der Erwägung, dass die rasante technologische Entwicklung die heimliche und nahezu nicht wahrnehmbare Beobachtung der Aktivitäten der Bürger im Internet immer mehr ermöglicht; in der Erwägung, dass allein die Tatsache, dass es Überwachungstechniken gibt, nicht automatisch deren Einsatz rechtfertigen darf, jedoch in der Erwägung, dass das vorrangige Interesse, die Grundrechte der Bürger zu schützen, entscheidend sein sollte bei der Festlegung der Grenzen und der genauen Umstände, unter denen solche Technologien von den Behörden oder von privaten Unternehmen verwendet werden dürfen;

H. in der Erwägung, dass darauf hingewiesen werden sollte, dass, wenn es um Rechte wie zum Beispiel freie Meinungsäußerung oder Achtung der Privatsphäre geht, eine Einmischung in die Ausübung dieser Rechte seitens der Behörden nur zulässig ist, wenn sie im Einklang mit „den geltenden Rechtvorschriften“ erfolgt und in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist;

I. in der Erwägung, dass im Internet, das seinem Wesen nach global, offen und partizipatorisch ist, in der Regel zwar Freiheit herrscht, dies dennoch nicht die Notwendigkeit ausschließt, darüber nachzudenken (auf nationaler und internationaler Ebene, im öffentlichen und im privaten Leben), wie sowohl die Grundfreiheiten der Internet-Nutzer als auch ihre Sicherheit geachtet und geschützt werden können;

J in der Erwägung, dass „Digibetismus“ (mangelnde Computer-Kenntnisse) der neue Analphabetismus des 21. Jahrhunderts ist; in der Erwägung, dass die Gewährleistung, dass alle Bürger Zugang zum Internet haben, daher gleichbedeutend damit ist, dass gewährleistet wird, dass alle Bürger Zugang zu Bildung haben, sowie in der Erwägung, dass dieser Zugang nicht durch Regierungen oder private Unternehmen zur Bestrafung verwehrt werden darf; in der Erwägung, dass dringende Fragen wie zum Beispiel Neutralität im Netz, Interoperabilität, weltweite Erreichbarkeit aller Internet-Knotenpunkte und Verwendung offener Formate und Standards unbedingt angegangen werden müssen;

K. in der Erwägung, dass die Wiederverwendung von Informationen des öffentlichen Sektors, die bisher nie da gewesene Möglichkeiten für kreative und kulturelle Experimente und Austausch bietet, und der Schutz der Rechte des geistigem Eigentums in einem ausgewogenen Verhältnis zueinander gehalten werden müssen;

1. richtet folgende Empfehlungen an den Rat:

Uneingeschränkter und sicherer Internetzugang für alle

(a) er möge sich an den Bemühungen beteiligen, das Internet zu einem wichtigen Instrument für Stärkung der Nutzer zu machen, zu einem Umfeld, das die Entwicklung von Vorgehensweisen „von unten“ und einer e-Demokratie ermöglicht und gleichzeitig sicherstellt, dass wichtige Schutzmechanismen geschaffen werden, da sich in diesem Bereich neue Formen der Kontrolle und der Zensur entwickeln können; Freiheit und Schutz der Privatsphäre der Internet-Nutzer sollte tatsächlich stattfinden und nicht nur vorgespiegelt werden;

(b) er möge anerkennen, dass das Internet eine außergewöhnliche Möglichkeit zur Förderung einer aktiven Bürgerschaft darstellen kann, und dass der Zugang zu Netzen und Inhalten in diesem Zusammenhang zu den wichtigsten Aspekten gehört, und empfehlen, dass dieser Themenkomplex weiter entwickelt wird, ausgehend von der Annahme, dass jeder das Recht hat, an der Informationsgesellschaft teilzunehmen, und dass Institutionen und Akteure auf allen Ebenen eine allgemeine Verantwortung dafür tragen, einen Beitrag zu dieser Entwicklung zu leisten, um so der doppelten Herausforderung der mangelnden Computerkenntnisse und der demokratischen Ausgrenzung im elektronischen Zeitalter zu begegnen;

(c) er möge gemeinsam mit anderen wichtigen Akteuren gewährleisten, dass Sicherheit, freie Meinungsäußerung und die Privatsphäre sowie Offenheit im Internet nicht als konkurrierende Ziele betrachtet, sondern gleichzeitig im Rahmen eines umfassenden Konzepts verfolgt werden, das all diesen Erfordernissen angemessen Rechnung trägt;

Entschlossenes Vorgehen bei der Bekämpfung der Cyber-Kriminalität

(d) er möge den Ratsvorsitz und die Kommission auffordern, über eine umfassende Strategie zur Bekämpfung der Cyber-Kriminalität nachzudenken, und unter anderem auch über Mittel und Wege, gegen das Problem des „Identitätsdiebstahls“ auf EU-Ebene vorzugehen;

(e) er möge zu Überlegungen über die notwendige Zusammenarbeit zwischen privaten und öffentlichen Akteuren in diesem Bereich und über die Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden anregen;

(f) er möge die Arbeit im Rahmen des Projekts „Check the Web“ fortsetzen und Maßnahmen zur Verbesserung der Verbreitung von Informationen über die Cyber-Kriminalität fördern, wie zum Beispiel die jüngsten Initiativen zur Einrichtung nationaler Plattformen und einer europäischer Plattform für Hinweise auf Internetstraftaten, soweit die nötigen Sicherheitsvorkehrungen getroffen sind;

(g) er möge Programme zum Schutz von Kindern und zur Aufklärung der Eltern über die neuen Gefahren des Internets fördern, wie im EU-Recht vorgesehen, und Folgeabschätzungen über die bisherige Wirksamkeit bestehender Programme vorlegen;

(h) er möge eine Richtlinie über strafrechtliche Maßnahmen zur Durchsetzung der Rechte des geistigen Eigentums annehmen und in diesem Zusammenhang gleichzeitig die systematische Beobachtung und Überwachung der Aktivitäten aller

Nutzer im Internet verbieten und gewährleisten, dass die Strafen im Verhältnis zu den begangenen Verstößen stehen; in diesem Zusammenhang auch das Recht auf freie Meinungsäußerung und die Vereinigungsfreiheit der einzelnen Benutzer achten und die Anstiftung zur Verletzung der Rechte des geistigen Eigentums im Internet bekämpfen, wozu auch bestimmte unverhältnismäßige Zugangseinschränkungen durch die Rechteinhaber selbst gehören;

(i) er möge gewährleisten, dass die Äußerung umstrittener politischer Überzeugungen im Internet, auch in Bezug auf Terrorismus, strafrechtlich nicht verfolgt wird;

Ständige Aufmerksamkeit für absoluten Schutz und verstärkte Förderung der Grundfreiheiten im Internet

(j) er möge der Tatsache Rechnung tragen, dass die „digitale Identität" zunehmend integraler Bestandteil unserer „Persönlichkeit" wird, und in diesem Sinne angemessen und wirksam vor Eingriffen privater und öffentlicher Akteure geschützt werden muss; der Bedeutung der Anonymität, der Pseudonymität und der Kontrolle der Informationsströme für die Privatsphäre gebührend Rechnung tragen sowie der Tatsache, dass den Nutzern die geeigneten Mittel an die Hand gegeben werden sollten, sich wirksam zu schützen;

(k) er möge die Gefahr verschiedener Formen von Internet-Beobachtung und -kontrolle erkennen, die darauf abzielen, jeden „digitalen Schritt" einer Person zu verfolgen, mit dem Ziel, ein Benutzerprofil zu erstellen und „Punkte" zuzuweisen; deutlich machen, dass solche Techniken immer nach ihrer Notwendigkeit sowie nach ihrer Verhältnismäßigkeit im Lichte der Ziele, die sie anstreben, beurteilt werden sollten; er möge auch die Notwendigkeit einer verbesserten Sensibilisierung der Nutzer betonen, damit sie ihre Zustimmung in Bezug auf ihre Aktivitäten im Internet (z. B. im Falle der sozialen Netze), erst dann geben, wenn sie genau wissen, was auf sie zukommt;

(l) er möge prüfen und festlegen, welche Grenzen es für die „Zustimmung" gibt, um die die Regierungen oder private Unternehmen die Nutzern bitten bzw. die sie von ihnen fordern können, damit einen Teil ihrer Privatsphäre aufgeben, da es ein deutliches Ungleichgewicht zwischen Verhandlungsposition und Wissensstand zwischen individuellen Nutzern und solchen Einrichtungen gibt;

(m) er möge die Fälle, in denen eine private Internetfirma aufgefordert werden kann, Daten an Regierungsbehörden weiterzugeben, rigoros begrenzen und festlegen;

(n) er möge Zensur durch die Regierung in Bezug auf Inhalte, nach denen im Internet gesucht werden kann, verurteilen, insbesondere wenn solche Einschränkungen eine „abschreckende Wirkung" auf politische Äußerungen haben können;

(o) er möge die Mitgliedstaaten auffordern, sicherzustellen, dass die freie Meinungsäußerung nicht willkürlichen Einschränkungen seitens der öffentlicher und/oder privater Einrichtungen unterliegt und alle Legislativ- oder Verwaltungsmaßnahmen vermeiden, die eine „abschreckende Wirkung" auf die Äußerungen einzelner Personen haben könnten;

(p) er möge darauf aufmerksam machen, dass die Entwicklung des „Internets der Dinge“ den Datenschutz und den Schutz der Rechte der Bürger nicht umgehen darf;

(q) er möge den Grundsatz „privacy by design“ („mit eingebautem Datenschutz“) fördern, wonach die Anforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz so bald wie möglich in den Lebenszyklus der neuen technologischen Entwicklungen eingebunden werden sollten;

Internationale Verpflichtungen

(r) er möge alle Internet-Akteure ermahnen, sich an dem laufenden Prozess der „Internet-Grundrechtecharta“ zu beteiligen, die auf jetzigen Grundrechten aufbaut, ihre Durchsetzung fördert und die Anerkennung neu entstehender Grundsätze vorantreibt; in diesem Zusammenhang muss die dynamische Koalition in Bezug auf die Internet-Grundrechtecharta eine führende Rolle spielen;

(s) er möge gewährleisten, dass in diesem Zusammenhang eine prozessorientierte Initiative mit vielen Beteiligten und auf zahlreichen Ebenen sowie eine Mischung zwischen globalen und lokalen Initiativen in Erwägung gezogen werden, um die Rechte der Internet-Nutzer genau festzulegen und zu schützen und auf diese Weise die Legitimität, die Rechenschaftspflicht und die Akzeptanz des Prozesses zu gewährleisten;

(t) er möge die aktive Teilnahme der EU an diversen internationalen Foren fördern, die sich mit den globalen und lokalen Aspekten des Internets befassen, zum Beispiel das Forums für Internet-Verwaltung (Internet Governance Forum – IGF);

(u) er möge gemeinsam mit allen relevanten Akteuren der EU an der Einrichtung eines europäischen IGF mitwirken, das eine Bilanz der Erfahrungen nationaler IGF ziehen, als regionaler Pol funktionieren und europaweite Fragen, Standpunkte und Anliegen in den neu entstehenden internationalen IGF effizienter vertreten würde;

o

o o

2. beauftragt seinen Präsidenten, diese Empfehlung dem Rat und, zur Information, der Kommission zu übermitteln.

11.6.2008

ENTWURF EINER EMPFEHLUNG AN DEN RAT (B6-0302/2008)

eingereicht gemäß Artikel 114 Absatz 1 der Geschäftsordnung

von Stavros Lambrinidis

zur Stärkung der Sicherheit und der Grundfreiheiten im Internet

Das Europäische Parlament,

– unter Hinweis auf die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten und auf die Charta der Grundrechte, insbesondere auf deren Artikel über den Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit sowie die Achtung des Privat- und Familienlebens,

– unter Hinweis auf die jüngsten Initiativen zur Aufdeckung von Fällen schwerer Kriminalität und von Terrorismus (Projekt „Check the web“) und den jüngsten Vorschlag zur Änderung des Rahmenbeschlusses 2002/475/JIA des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung sowie den Vorschlag zur Überarbeitung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation,

– unter Hinweis auf die Arbeiten beim Europarat, bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und bei den Vereinten Nationen sowohl in Bezug auf die Bekämpfung der Kriminalität und der Internetkriminalität als auch in Bezug auf den Schutz der Grundrechte und Grundfreiheiten auch im Internet,

– unter Hinweis auf die jüngsten diesbezüglichen Urteile der europäischen Gerichte und der nationalen Verfassungsgerichte, insbesondere das Urteil des Bundesverfassungsgerichts, das ein eigenes Recht auf Schutz der Vertraulichkeit und Integrität der EDV-Systeme anerkennt,

– gestützt auf Artikel 114 Absatz 1 seiner Geschäftsordnung,

A. in der Erwägung, dass das Internet weltweit zu einem wesentlichen Instrument für die Entwicklung der Meinungsfreiheit und für die Entfaltung der wirtschaftlichen Tätigkeiten geworden ist; in der Erwägung ferner, dass es in diesem Zusammenhang in besonderer Weise darauf ankommt, dass die Bekämpfung der Kriminalität und von Missbräuchen durch die öffentliche Hand oder durch Einzelpersonen das Potenzial dieses Instrumentes nicht einschränkt,

B. in der Erwägung, dass das Phänomen Internet auf Grund seiner weltweiten Ausrichtung, seiner raschen Entwicklung und seiner technischen Besonderheiten nur schwer durch das alleinige nationale Recht gefasst werden kann und dass insbesondere auf internationaler Ebene Initiativen zum Schutz der Rechte des Einzelnen ergriffen werden sollten, und zwar

sowohl zum Schutz der Rechte, die die Sicherheit des Einzelnen betreffen, als auch jener, die die Freiheiten des Einzelnen schützen, als auch jener, die den Schutz der Privatsphäre betreffen,

1. richtet folgende Empfehlungen an den Rat, mit denen die Voraussetzungen zur Erreichung der nachstehend aufgeführten Ziele geschaffen werden sollen:

   a) Ermöglichung einer allmählichen Annäherung der einzelstaatlichen Rechtsvorschriften innerhalb der EU in Bezug auf die Anforderungen im Zusammenhang mit dem Schutz der Grundrechte im Internet,

   b) Intensivierung des Dialogs zwischen den nationalen und europäischen Gesetzgebern sowie zwischen den nationalen und den europäischen Gerichtsbarkeiten,

   c) Förderung des Dialogs zwischen allen implizierten und vom Phänomen Internet betroffenen Akteuren, insbesondere die Internet-Operateure und die Anwender,

   d) Förderung des Abschlusses der notwendigen Abkommen auf internationaler Ebene, sowohl bilateral (insbesondere im Rahmen der transatlantischen Beziehungen) als auch multilateral (Initiativen des Europarats, der OECD und der UNO);

2. beauftragt seinen Präsidenten, diese Empfehlung dem Rat und – zur Kenntnisnahme – der Kommission zu übermitteln.

BEGRÜNDUNG

Grundrechte im Internet – eine Verbesserung bei gleichzeitiger Gefährdung

Wir leben in einem Zeitalter, in dem jeder einen möglichst umfassenden Zugang zu unseren persönlichen elektronischen Daten anstrebt: Regierungen, Polizei, Privatunternehmen und sogar Kriminelle. Insbesondere das Internet bietet einen bisher nicht vorstellbaren Einblick über Einzelheiten unseres Privatlebens; nur ein einziger Klick auf eine Webseite gibt Daten frei, die potenziell von Werbetreibenden, Nachrichtendiensten oder Identitätsdieben benutzt bzw. missbraucht werden können.

Daher gehört die Gewährleistung des Schutzes des **Grundrechts auf Privatsphäre** im Internet zu den dringlichsten Aufgaben, mit denen wir als Gesetzgeber konfrontiert werden. Sie ist auch eine der heikelsten ethischen, juristischen, technologischen und politischen Herausforderungen, denen sich unsere Gesellschaften je gegenüber sahen.

Es ist jedem klar, dass das Internet ein Instrument zur Erweiterung unserer Grundrechte sein kann, das uns mit grenzenlosen Informationen versorgt und uns mit Einzelpersonen und Gemeinschaften in der ganzen Welt verbindet. Etwas weniger bekannt ist die Tatsache, dass das Internet dabei auch unsere Grundrechte ernsthaft gefährdet und uns potenziell böswilliger Überwachung aussetzt und Kriminellen und sogar Terroristen als Mittel dient. Und am wenigsten ist klar, wie wir das Internet so regulieren können, dass wir die Vorteile nutzen und gleichzeitig die sehr realen und ernsthaften Risiken des Missbrauchs begrenzen können. Diese Rechnung wird auch noch durch das Internet selbst kompliziert – ein seinem Wesen nach dezentralisiertes, von den Nutzern gestaltetes Netz, das keiner staatlichen Kontrolle unterliegt und das nahezu alle Grenzen überschreitet.

Mit diesem Bericht soll daher darauf hingewiesen werden, wie wir die grundlegenden Freiheiten des Individuums in einem Online-Umfeld am besten schützen und fördern können. Vor allem sollten wir folgende Maßnahmen treffen:

– alle Akteure einbinden;
– auf unterschiedlichen Ebenen tätig werden, vorhandene nationale, regionale und internationale Instrumente nutzen und beobachten, wie diese in der geltenden legislativen Praxis umgesetzt werden;
– bewährte Verfahren austauschen, und
– den Bedürfnissen und Problemen unterschiedlicher Internet-Nutzer und vieler (und sich ständig weiter entwickelnder) Ausprägungen von Online-Tätigkeiten Rechnung tragen.

Die Suche nach dem richtigen Gleichgewicht zwischen Privatsphäre und Sicherheit steht im Mittelpunkt unserer Aufgabe. Sie bedarf der ständigen Wachsamkeit und Feinabstimmung, damit wir mit dem unaufhaltsamen Fortschritt der Technologie Schritt halten. Wir müssen sorgfältig Sicherheitsanliegen jeglicher Art prüfen, von Fragen der nationalen Sicherheit über die Sicherheit und Zuverlässigkeit unserer Netze bis hin zur persönlichen Sicherheit von Individuen, wenn sie ihre Daten online zugänglich machen. Für ein sichereres Internet zu sorgen, ist ein legitimes Ziel für unsere Gesellschaft, wir müssen aber den Einsatz von Beobachtungs- und Überwachungstechniken, die unsere Grundfreiheiten gefährden könnten,

überprüfen und einschränken, insbesondere, wenn deren Notwendigkeit, Verhältnismäßigkeit und Wirksamkeit in Frage gestellt werden können. Flexibilität, Anpassungsfähigkeit und Rechenschaftspflicht müssen die Eckpfeiler aller Rechtsvorschriften und Programme sein, die wir ausarbeiten, damit wir den sich entwickelnden Technologien immer einen Schritt voraus sein können.

Das Internet kann auch wesentlich zu einer Stärkung anderer Grundrechte, wie der Redefreiheit, des Rechts auf politische Tätigkeit und der Vereinigungsfreiheit, beitragen, es kann diese Rechte aber ebenso gut aushöhlen. Ein jüngstes Beispiel in dieser Debatte war die legislative Initiative zur Überwachung von Beiträgen im Internet zur Vermeidung von Terroranschlägen. Dies ist ein klassisches Beispiel für Rechtsvorschriften, die, wenn sie nicht genau auf die jeweiligen Ziele zugeschnitten werden, der umfassenden Überwachung Tür und Tor öffnen und so Individuen von politischer Meinungsäußerung abhalten könnten, obwohl diese doch wesentlicher Bestandteil einer demokratischen Gesellschaft sind.

Es ist entscheidend, hier das richtige Gleichgewicht zu finden. Es steht außer Frage, dass das Internet Kriminellen ein leistungsfähiges neues Instrumentarium an die Hand gegeben hat, und es ist selbstverständlich, zu vermeiden, dass Terroristen das Internet benutzen, um Anschläge zu planen und durchzuführen. Ebenso fordert unsere Gesellschaft zu Recht, dass wir gegen die für Kinderpornographie im Internet Verantwortlichen vorgehen. Durch solche Kriminelle, die eine spürbare Bedrohung darstellen, werden die Hemmschwellen der Bürger in Bezug auf Forderungen an die Polizei nach einer umfassenden Überwachung des Internets, das aufgrund seiner Wesensart „nicht greifbar“ ist, herabgesetzt. Wir müssen dieser Tendenz widerstehen. Unsere Gesetze müssen das Verbrechen wirksam bekämpfen, dürfen aber nicht unverhältnismäßig sein. Durch seine eher amorphe und ungreifbare Art leistet das Internet von sich aus solchen Unverhältnismäßigkeiten Vorschub. Zum Beispiel würden nur wenige Menschen es hinnehmen, dass die Polizei oder Marketingfirmen jedes mit der Post verschickte Schreiben öffnen, um dessen Inhalt zu prüfen. Eine ähnliche Wachsamkeit ist erforderlich, wenn es um den Schutz des Inhalts elektronischer Mitteilungen geht.

Jedoch können nicht nur Regierungsbehörden im Rahmen der Verfolgung von Verbrechern, sondern auch private Internetfirmen beim Gewinnstreben eine abschreckende Wirkung auf die Redefreiheit haben oder die Privatsphäre beeinträchtigen. Die neueste Tendenz, besteht darin, und in der Regel nur, nachdem Firmen auf frischer Tat beim Einholen, beim Speichern und bei der Verwendung unserer Daten ohne Genehmigung ertappt wurden, den Nutzer um **„Zustimmung“** (entweder auf einer Opt-in- oder einer Opt-out-Basis) zur Verwendung seiner Daten zu bitten, aber nur, wenn es überhaupt herauskommt.

Wir müssen uns fragen: **„Wo liegen die Grenzen unserer Zustimmung?“** Diese Frage gilt sowohl in Bezug auf das, was ein Unternehmen von uns an Offenlegung verlangen kann, und wie viel ein Individuum von seiner Privatsphäre und anderen Grundrechten preisgeben darf, um bestimmte Internetdienste oder -vorteile zu bekommen.

Die Antworten auf diese Fragen sind nicht so einfach. In einem anderen Bereich, dem Bereich des Arbeitsrechts, ist unsere Gesellschaft zu der Schlussfolgerung gelangt, dass es Grenzen gibt bei der Zustimmung der Bürger in Bezug auf ihr Privatleben. So legen das Arbeitsrecht und die Tarifvereinbarungen in den meisten Mitgliedstaaten zum Beispiel die

Höchstarbeitszeit, den Mindestlohn oder andere Arbeitnehmerrechte fest, und es kann von Einzelpersonen nicht verlangt werden, dass sie diese Rechte mit ihren Arbeitgebern „wegverhandeln“. Hierfür gibt es einen einfachen Grund: Es wird davon ausgegangen, dass es kein ausgewogenes Kräfteverhältnis zwischen Arbeitnehmer und Arbeitgeber gibt, und dass „Zustimmung” daher wohl kaum auf einer Basis der Gleichheit gegeben werden kann. Ein weiterer Grund besteht darin, dass wir ebenfalls beschlossen haben, dass wir einen „Wettlauf nach unten“ bei allen Arbeitnehmerrechten vermeiden müssen, zu dem es kommen könnte, wenn einigen Arbeitnehmern auf individueller Basis gestattet würde, einige ihrer Rechte durch Verhandlungen aufzugeben oder wenn sie dazu gezwungen würden.

Eine vergleichbare Macht- und Wissenslücke existiert im Internet. Die Macht, das Wissen und die Interessen von Unternehmen und der Regierung haben die Oberhand über den einzelnen Nutzer, und ebenso das Risiko, “billigere“ (und daher für einige Nutzer attraktivere) Internetdienste anzubieten, dafür aber einen geringeren Schutz der Privatsphäre sicherzustellen. Bei der nächsten Schlacht im Rahmen der Debatte über Sicherheit und Privatsphäre im Internet wird es zweifellos um die Grenzen der „Zustimmung“ gehen, die Regierungen und private Firmen verlangen.

Diese Frage muss uns beschäftigen, denn im heutigen Europa kommt „Big Brother“ nicht in Form irgendeines autoritären Regimes daher; wenn die totale Überwachung kommt, kommt sie auf leisen Sohlen und ohne unsere „Zustimmung“.

Schließlich sind **das Recht auf Bildung und das Recht auf Zugang zum Internet** zwei zusätzliche Rechte, die als eigenständige Rechte gefördert werden müssen, die aber im Rahmen der Bekämpfung der Kriminalität über das Internet bedroht sein könnten. Mangelnde Computerkenntnisse werden zum neuen Analphabetismus des 21. Jahrhunderts. Da jedes Kind heute ein Recht auf Schulunterricht und jeder Erwachsene ein Recht auf Fortbildung hat, sollte jede Person ihr ganzes Leben lang das Recht auf Zugang zu Computern und zum Internet haben. Die Regierungen sollten diesen Zugang auch für die am weitesten abgelegenen Regionen des Landes und für ihre ärmsten Bürger sicherstellen; darüber hinaus darf dieses Recht nicht zur „Strafe“ den Bürgern verwehrt werden, wenn sie gegen das Gesetz verstoßen haben. Menschen aus allen sozialen Schichten und aus allen Regionen und Kulturen sollten in der Lage sein, die breite Vielfalt der im Internet angebotenen Dienstleistungen zu nutzen. So können sie sich entfalten, bildungsspezifische, berufliche und persönliche Beziehungen eingehen und wirtschaftliche Gelegenheiten, die unsere Technologien und unsere Gesetze bieten, voll ausschöpfen.