DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien

(2009/C 2/02)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

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

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

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ([2]), insbesondere auf Artikel 41,

gestützt auf das am 4. März 2008 eingegangene Ersuchen der Europäischen Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. **EINLEITUNG**

Konsultation des EDSB

1. Der Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien (nachstehend „Vorschlag" genannt) ist dem EDSB durch die Kommission am 4. März 2008 zur Stellungnahme gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 übermittelt worden. Diese Stellungnahme sollte in der Präambel des Beschlusses ausdrücklich erwähnt werden.

Hintergrund des Vorschlags

2. Das neue mehrjährige Programm (nachstehend „Programm" genannt) wird als Folgeprogramm zu den Programmen „Sicherheit im Internet" (1999-2004) und „Mehr Sicherheit im Internet" (2005-2008) vorgeschlagen.

3. Vier Zielvorgaben sind darin festgelegt worden:

   — Verringerung illegaler Inhalte und Bekämpfung schädlichen Verhaltens im Online-Umfeld,

   — Förderung eines sichereren Online-Umfelds,

   — Sensibilisierung der Öffentlichkeit,

   — Aufbau einer Wissensbasis.

4. Es wird erklärt, dass das Programm mit den bereits bestehenden Maßnahmen, Programmen und Aktionen der Gemeinschaft im Einklang steht und diese ergänzt. In Anbetracht der Zahl bereits bestehender Rechtsetzungsmaßnahmen auf dem Gebiet des Schutzes von Kindern im Zusammenhang mit neuen Technologien konzentriert sich dieses Programm auf Aktionen und nicht auf Rechtsetzung. Im Mittelpunkt stehen die Effizienz und Wirksamkeit der durchzuführenden Initiativen und die Anpassung an die Fortentwicklung neuer Technologien. Das Programm sieht daher einen verbesserten Austausch von Informationen und bewährten Verfahren vor.

5. Da es sich um ein Rahmeninstrument handelt, wird in dem Programm nicht auf die Einzelheiten der Aktionen eingegangen, aber es ermöglicht Aufforderungen zur Einreichung von Vorschlägen und Ausschreibungen gemäß den vier Zielvorgaben.

Schwerpunkt der Stellungnahme

6. Die allgemeinen Zielvorgaben des Programms betreffen den Schutz des Kindes bei der Nutzung des Internets und anderer Kommunikationstechnologien, ohne dass die diesbezüglichen Datenschutzaspekte herausgestellt werden ([3]). Der EDSB befürwortet voll und ganz die Zielsetzung des Vorschlags, wird in dieser Stellungnahme aber die Datenschutzaspekte herausstellen.

([1]) ABl. L 281 vom 23.11.1995, S. 31.
([2]) ABl. L 8 vom 12.1.2001, S. 1.

([3]) Einige Bezüge zum Datenschutz finden sich in der Folgenabschätzung (3.2. Besondere Risiken: Preisgabe persönlicher Informationen; 3.3. Zielgruppen; 5.2. Analyse der Auswirkungen der Handlungsoptionen), werden aber nicht näher ausgeführt.

7. Nach Auffassung des EDSB ist es unerlässlich, dass die geplanten Initiativen mit dem geltenden Rechtsrahmen, wie er im Vorschlag zitiert wird ([1]), und insbesondere der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr, der Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation und der Richtlinie 95/46/EG über Datenschutz ([2]) im Einklang stehen.

8. Der Schutz personenbezogener Daten sollte in Bezug auf unterschiedliche Aspekte und Akteure, die mit dem Programm im Zusammenhang stehen, Berücksichtigung finden: dabei ist der Schutz personenbezogener Daten von Kindern natürlich das wichtigste Thema, aber nicht das einzige; personenbezogene Daten in Bezug auf Personen und Inhalt, die für den Zweck des Schutzes von Kindern relevant sind, sollten ebenfalls berücksichtigt werden.

9. Diese Aspekte werden in dieser Stellungnahme wie folgt behandelt:

   — in Kapitel II wird auf den Bezug zwischen Datenschutz und Sicherheit des Kindes eingegangen und es wird darauf hingewiesen, dass der Schutz personenbezogener Daten von Kindern ein notwendiger Schritt auf dem Weg zu mehr Sicherheit und Schutz vor Missbrauch ist,

   — in Kapitel III der Stellungnahme wird herausgestellt, dass auch bei der Meldung, beim Herausfiltern oder beim Sperren verdächtiger Inhalte oder Personen im Internet personenbezogene Daten verarbeitet werden:

      — in einem ersten Abschnitt wird die Frage der Meldung verdächtiger Personen oder Sachverhalte unter dem Blickwinkel des Datenschutzes analysiert,

      — im Mittelpunkt des zweiten Abschnitts steht die Rolle technischer Instrumente,

      — die Verantwortung der Branche in Bezug auf ihre Kontrolle über Nutzerdaten und Inhalte wird im letzten Abschnitt behandelt.

II. SCHUTZ PERSONENBEZOGENER DATEN UND SICHERHEIT DES KINDES

10. Der EDSB unterstützt voll und ganz die Zielsetzung des Programms und die Vorgaben zur Verbesserung des Schutzes von Kindern im Online-Umfeld. Insbesondere die Verringerung illegaler oder schädlicher Inhalte und die Sensibilisierung von Kindern und anderen Beteiligten sind entscheidende Maßnahmen, die weiterentwickelt werden sollten.

11. Der EDSB möchte darauf hinweisen, dass ein angemessener Schutz der personenbezogenen Daten des Kindes ein unerlässlicher erster Schritt ist, um die Sicherheit während der Nutzung des Internets zu gewährleisten. Dieser Zusammenhang zwischen Datenschutz und Sicherheit des Kindes wird in der letzten Erklärung des Ministerkomitees des Europarates über den Schutz der Würde, der Sicherheit und der Daten von Kindern bei der Nutzung des Internets ([3]) ausdrücklich erwähnt. In der Erklärung wird auf das Recht des Kindes auf Würde, besonderen Schutz und Fürsorge, wie sie für das Wohl des Kindes erforderlich sind, sowie auf Schutz vor allen Formen der Diskriminierung oder vor der willkürlichen oder unrechtmäßigen Verletzung der Privatsphäre und vor unrechtmäßigen Angriffen auf seine Ehre und sein Ansehen hingewiesen.

12. Als Beispiel für Risiken im Zusammenhang mit dem Schutz der Privatsphäre von Kindern wird in der Erklärung die Rückverfolgbarkeit der Internetaktivitäten von Kindern genannt, die Kinder zum Ziel krimineller Handlungen machen kann, beispielsweise durch Anstiftungen mit sexuellem Hintergrund oder andere illegale Aktivitäten. Ferner wird erläutert, dass das Profiling und die Speicherung personenbezogener Daten zum Nutzerverhalten von Kindern eine mögliche Gefahr des Missbrauchs beispielsweise zu kommerziellen Zwecken oder für Recherchen von Bildungseinrichtungen oder potenziellen Arbeitgebern bergen. In der Erklärung wird daher gefordert, dass von Kindern generierte Inhalte und Spuren, die Kinder bei der Nutzung des Internets hinterlassen, innerhalb eines angemessen kurzen Zeitraums entfernt oder gelöscht werden und dass die Aufklärung von Kindern insbesondere über die kompetente Nutzung von Werkzeugen für den Zugang zu Informationen, die kritische Analyse von Inhalten und die Aneignung adäquater Kommunikationsfähigkeiten weiterentwickelt und gefördert werden.

13. Der EDSB schließt sich diesen Aussagen an. Er betrachtet es insbesondere als entscheidend, Kinder über die Risiken aufzuklären, die bei der spontanen Weitergabe persönlicher Angaben wie des wirklichen Namens, des Alters oder des Wohnortes bestehen.

14. Abschnitt 3 der mit dem Mehrjahresprogramm vorgeschlagenen Aktionen ([4]) gilt der „Sensibilisierung der Öffentlichkeit"; dazu gehören Maßnahmen, die auf Kinder, Eltern, Betreuer und Erzieher abstellen und die Chancen und Risiken, die sich aus der Nutzung der Online-Technologien ergeben, und die Mittel und Wege eines sicheren Verhaltens im Online-Umfeld betreffen. Die Verbreitung geeigneter Informationen und die Einrichtung von Anlaufstellen, bei denen Eltern und Kinder Antworten auf ihre Fragen zur sicheren Internetnutzung erhalten, sind zwei bedeutende der in dem Vorschlag aufgeführten Instrumente, bei denen der Aspekt des Schutzes personenbezogener Daten des Kindes eine Rolle spielen sollte.

15. Der EDSB möchte betonen, dass die Datenschutzbehörden in diesem Zusammenhang wichtige Gesprächspartner sind. Sie sollten in dem Vorschlag eigens erwähnt werden, und zwar insbesondere dort, wo der Vorschlag die Förderung der Zusammenarbeit sowie des Austauschs von Informationen, Erfahrungen und empfehlenswerten Verfahren zwischen den Akteuren auf nationaler und europäischer Ebene vorsieht ([5]).

([1]) Begründung, 2.1. Rechtlicher Hintergrund; Zusammenfassung der Folgenabschätzung, 1.2. Aktueller Stand: Rechtsvorschriften.

([2]) — Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000, S. 1,
— 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,
— 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, ABl. L 281 vom 23.11.1995, S. 31.

([3]) Erklärung des Ministerkomitees des Europarates vom 20. Februar 2008 auf der 1018. Tagung des Komitees auf Stellvertreterebene, abrufbar unter „wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.2.2008)&Ver=0001".

([4]) Abschnitt 3 (Aktionen).

([5]) Anhang 1 Abschnitt 1 (Aktionen).

16. Mehrere Initiativen können zur Verdeutlichung der Maßnahmen angeführt werden, die in jüngster Zeit in den Mitgliedstaaten oder von Mitgliedern des EWR in dieser Hinsicht ergriffen wurden. Die schwedische Datenschutzbehörde führt jährlich eine Umfrage zur Einstellung junger Menschen zum Thema Internet und Überwachung durch, ebenso wie die Datenschutzbehörde des Vereinigten Königreichs ([1]), die 2 000 Jugendliche im Alter von 14 bis 21 Jahren befragt hat. Die norwegische Datenschutzbehörde hat im Januar 2007 zusammen mit dem Bildungsministerium eine Aufklärungskampagne für Schulen durchgeführt ([2]). In Portugal ist zwischen der Datenschutzbehörde und dem Bildungsministerium ein Protokoll unterzeichnet worden, das darauf abzielt, eine Datenschutzkultur im Internet und insbesondere auf Social-Networking-Websites zu fördern ([3]). In diesem Rahmen haben portugiesische Social-Networking-Websites eine Schnittstelle und ein Maskottchen speziell für Kinder im Alter von 10 bis 15 Jahren eingeführt.

17. Diese Beispiele verdeutlichen die aktive und entscheidende Funktion von Datenschutzbehörden, wenn es um den Schutz von Kindern im Online-Umfeld geht, und zeigen, wie wichtig es ist, Datenschutzbehörden explizit im Mehrjahresprogramm als Gesprächspartner aufzuführen.

III. SCHUTZ PERSONENBEZOGENER DATEN UND RECHTE ANDERER BETEILIGTER

I. *Meldungen und Informationsaustausch*

18. Im ersten Abschnitt des Vorschlags („Verringerung illegaler Inhalte und Bekämpfung schädlichen Verhaltens im Online-Umfeld“ ([4])) ist als eine der wichtigsten Aktionen vorgesehen, öffentliche Anlaufstellen für die Meldung illegaler Inhalte und schädlichen Verhaltens im Online-Umfeld einzurichten. Es ist unbestritten, dass illegale Inhalte und schädliches Verhalten den zuständigen Behörden gemeldet werden müssen, damit wirksam dagegen vorgegangen werden kann. Es sind bereits Anlaufstellen für den Schutz von Kindern, aber beispielsweise auch für den Schutz vor Spam-Nachrichten ([5]) eingerichtet worden.

19. Der EDSB weist indessen darauf hin, dass der Begriff schädlicher Inhalt nach wie vor nicht klar umrissen ist: Es wird nicht angegeben, wer dafür zuständig ist, zu definieren, was unter schädlichem Inhalt zu verstehen ist und nach welchen Kriterien dies erfolgt. Dies ist umso beunruhigender, wenn man die Auswirkungen einer möglichen Meldung solcher Inhalte betrachtet.

20. Darüber hinaus geht es wie bereits erwähnt in einem Programm wie diesem nicht nur um die personenbezogenen Daten von Kindern, sondern um die personenbezogenen Daten aller, die auf irgendeine Weise eine Verbindung zu den Informationen aufweisen, die im Internet kursieren. Dabei kann es sich beispielsweise um die Person handeln, die eines Fehlverhaltens verdächtigt wird und als Verdächtiger gemeldet wird, aber auch um die Person, die ein verdächtiges Verhalten oder einen verdächtigen Inhalt meldet, oder um den Missbrauchsgeschädigten. Diese Daten sind zwar für ein wirksames Meldesystem erforderlich, aber der EDSB hält es für wichtig, darauf hinzuweisen, dass sie stets im Einklang mit den Grundsätzen des Datenschutzes verarbeitet werden sollten.

21. Für einige Daten kann sogar ein spezifischer Schutz erforderlich sein, wenn sie als sensible Daten im Sinne von Artikel 8 der Richtlinie 95/46/EG betrachtet werden können. Dies kann bei Daten zu Tätern und bei Missbrauchsopfern der Fall sein, insbesondere wenn es um Kinderpornographie geht. Es sei darauf hingewiesen, dass auf nationaler Ebene für einige Meldesysteme Änderungen der Datenschutzgesetze erforderlich waren, um die Verarbeitung justizieller Daten von Tatverdächtigen oder von Opfern zu ermöglichen ([6]). Der EDSB weist darauf hin, dass bei jedem Meldesystem, das eingerichtet werden soll, der geltende Datenschutzrahmen berücksichtigt werden muss. Der Nachweis eines öffentlichen Interesses sowie Garantien hinsichtlich der Überwachung des Systems, die grundsätzlich durch Strafverfolgungsbehörden zu erfolgen hat, sind entscheidende Faktoren für die Einhaltung der rechtlichen Vorschriften im Rahmen des Datenschutzes..

II. *Die Rolle technischer Instrumente aus der Datenschutzperspektive*

22. Der Einsatz technischer Instrumente wird als eine der Lösungen für das Vorgehen gegen illegale Inhalte und schädliches Verhalten befürwortet ([7]). Beispiele hierfür werden in der Folgenabschätzung gegeben ([8]); dazu gehören die Alterserkennung, die Gesichtserkennung (für die Opferidentifizierung durch Strafverfolgungsbehörden) oder Filtertechnologien. Dem Vorschlag zufolge sollten diese Instrumente besser an die praktischen Bedürfnisse angepasst werden und für die entsprechenden Akteure zur Verfügung stehen.

23. Der EDSB hat sich bereits deutlich für die Nutzung neuer Technologien zur Verbesserung des Schutzes der Rechte von natürlichen Personen ausgesprochen ([9]). Er ist der Auffassung, dass der Grundsatz „privacy by design“ (mit eingebautem Datenschutz) ein fester Bestandteil technologischer Entwicklungen, die die Verarbeitung personenbezogener Daten zur Folge haben, sein sollte. Der EDSB befürwortet daher entschieden die Entwicklung von Projekten, die auf die Entwicklung entsprechender Technologien abzielen.

24. Es ist besonders wichtig, dass Systeme entwickelt werden, die die Offenlegung personenbezogener Daten von Kindern so weit wie möglich verringern, Kindern einen zuverlässigen Schutz bieten und ihnen dementsprechend die Möglichkeit bieten, neue Instrumente der Informationsgesellschaft wie Social-Networking-Websites sicherer zu nutzen.

([1]) Siehe Anhang 1 „www.ico.gov.uk/youngpeople“.
([2]) Siehe „www.dubestemmer.no“.
([3]) Siehe „dadus.cnpd.pt/“.
([4]) Anhang 1 des Vorschlags.
([5]) Siehe beispielsweise die entsprechende Website der belgischen Behörden: www.ecops.be
([6]) Siehe das belgische Datenschutzgesetz vom 8. Dezember 1992, Artikel 3 Absatz 6 zur Datenverarbeitung durch das Zentrum für die Meldung vermisster oder sexuell missbrauchter Kinder.
([7]) Anhang 1 Abschnitt 1 (Aktionen).
([8]) Folgenabschätzung, Abschnitt 3.1.
([9]) Jahresbericht 2006 des EDSB, Abschnitt 3.5.1 „Technologische Entwicklungen“.

25. Es sei jedoch darauf hingewiesen, dass technische Mittel, je nachdem wie sie genutzt werden, eine Reihe von Auswirkungen auf den Einzelnen haben können. Wenn sie eingesetzt werden, um Informationen zu filtern oder zu sperren, kann damit zwar der Zugang von Kindern zu möglicherweise schädlichen Inhalten, aber auch der Zugriff auf rechtmäßige Informationen verhindert werden.

26. Auch wenn es dabei in erster Linie um den freien Zugang zu Informationen geht, ergibt sich dennoch eine Konsequenz aus der Datenschutzperspektive. Datenfilterung kann nämlich insbesondere bei den jüngsten Entwicklungen, bei denen ein Identitätsmanagement eingesetzt wird, auf der Grundlage bestimmter Kriterien funktionieren, zu denen personenbezogene Daten wie das Alter der Netzteilnehmer (um zu verhindern, dass Erwachsene oder Kinder Zugang zu spezifischen Inhalten haben), der Inhalt der Daten und Verbindungsdaten im Zusammenhang mit der Identität des Datenurhebers gehören. Je nachdem, wie diese personenbezogenen Daten — automatisch — verarbeitet werden, könnte sich dies für die Betroffenen auf ihr Recht auf Online-Kommunikation auswirken.

27. Die Nutzung von Filtern oder Sperren zur Kontrolle des Zugangs zu Netzwerken muss daher umsichtig erfolgen, so dass die eventuellen gegenteiligen Auswirkungen berücksichtigt und die Möglichkeiten dieser Technik für die Verbesserung des Datenschutzes voll und ganz ausgeschöpft werden.

28. Der EDSB begrüßt die Präzisierung in der Folgenabschätzung ([1]), dass keine der vorgeschlagenen Möglichkeiten das Recht auf Privatsphäre und auf freie Meinungsäußerung beeinträchtigen sollte. Er teilt ferner die dort zum Ausdruck gebrachte Sichtweise, dass eines der wichtigsten Ziele die Stärkung der Handlungskompetenz der Nutzer ist, d. h. die Befähigung zu besseren Entscheidungen und zur Durchführung geeigneter Maßnahmen für den Schutz von Kindern ([2]).

III. *Die Verantwortung von Diensteanbietern*

29. Entsprechend des Vorschlags ist die Mitwirkung aller Akteure ein notwendiger Faktor für die Verbesserung des Schutzes von Kindern bei der Nutzung von Kommunikationstechnologien. Der Vorschlag ([3]) sieht dabei die Beteiligung und die Einbeziehung der Branche — als einer der Akteure — vor, und zwar insbesondere durch Selbstregulierung.

30. Da die Branche für die Bereitstellung von Telekommunikations- und Inhaltediensten zuständig ist, könnte sie gewissen Einfluss auf die Meldung, Filterung oder Sperrung von Informationen haben, die als illegal oder schädlich betrachtet werden. Das Ausmaß, in dem der Branche tatsächlich eine solche Aufgabe übertragen werden kann, könnte jedoch aus rechtlicher Sicht zu Diskussionen führen.

31. Die Mitwirkung der Branche bei der Sensibilisierung von Kindern und anderen Akteuren wie Eltern oder Erziehern ist natürlich willkommen. Die Einrichtung von Alarmsystemen und die Einschaltung von Moderatoren auf Websites, die den Ausschluss ungeeigneter Inhalte ermöglichen, ist ebenfalls ein wichtiger Aspekt der Verantwortlichkeit der Inhalteanbieter.

32. Was die Anbieter von *Telekommunikations*diensten anbelangt, ist die Überwachung der Telekommunikationsdienste indessen eine strittige Frage, die entweder auf die Überwachung von urheberrechtlich geschützten Inhalten oder auf die Überwachung von illegalen Inhalte abstellt. Dabei wird die Frage des Eingreifens eines Wirtschaftsteilnehmers, der einen spezifischen (Telekommunikations-)Dienst anbietet, in diesem Bereich aufgeworfen, in dem er grundsätzlich nicht eingreifen sollte, nämlich im Bereich der inhaltlichen Kontrolle der Telekommunikationsdienste. Der EDSB weist darauf hin, dass eine derartige Kontrolle grundsätzlich nicht durch Diensteanbieter und sicherlich auch nicht systematisch erfolgen sollte. Ist eine Kontrolle unter bestimmten Umständen erforderlich, so sollte sie grundsätzlich Aufgabe der Strafverfolgungsbehörden sein.

33. In ihrer Stellungnahme vom 18. Januar 2005 hat die Datenschutzgruppe „Artikel 29" zu dieser Frage erklärt ([4]), „dass die Internetdienstanbieter gemäß Artikel 15 der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr nicht systematisch zur Überwachung oder Zusammenarbeit verpflichtet (werden können). (…) Gemäß Artikel 8 Absatz 5 der Datenschutzrichtlinie darf die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, nur unter strengen, von den Mitgliedstaaten festgelegten Voraussetzungen erfolgen. Wenngleich dem Einzelnen zweifelsohne das Recht zusteht, Strafverfolgungsdaten im Rahmen eines eigenen Rechtsstreits zu verarbeiten, so geht der Grundsatz doch nicht so weit, dass er die gründliche Ermittlung, Erfassung und Zentralisierung personenbezogener Daten durch Dritte erlauben würde, wozu auch generelle systematische Ermittlungen wie das Durchforsten des Internets (Internet-Scanning) zählen (…). Derartige Ermittlungen sind Sache der Strafverfolgungsbehörden."

34. In einem Bereich, in dem es um freie Meinungsäußerung, Zugang zu Informationen, Recht auf Privatsphäre und andere Grundrechte geht, wird durch das Eingreifen privater Akteure die Frage der Verhältnismäßigkeit der Mittel aufgeworfen. Das Europäische Parlament hat unlängst in einer Entschließung betont, dass es einer Lösung bedarf, bei der die Grundrechte der Bürger gewahrt bleiben ([5]). Unter Nummer 23 der Entschließung erklärt das Europäische Parlament, dass „das Internet eine breite Plattform für die kulturelle Ausdrucksmöglichkeit, den Zugang zu Wissen und die demokratische Teilhabe an der europäischen Kreativität darstellt und die Generationen durch die Informationsgesellschaft zusammenbringt; (das Parlament) fordert die Kommission und die Mitgliedstaaten daher auf, keine Maßnahmen zu ergreifen, die im Widerspruch zu den bürgerlichen Freiheiten und den Menschenrechten sowie den Grundsätzen der Verhältnismäßigkeit, der Effizienz und der Abschreckung stehen, wie z. B. die Unterbrechung des Internet-Zugangs".

([1]) Folgenabschätzung, Abschnitt 5.2.

([2]) In diesem Sinne sollten Filter von den Eltern aktiviert und auch wieder deaktiviert werden können, so dass die Erwachsenen voll und ganz die Kontrolle über die Filterfunktion behalten.

([3]) Erwägungsgrund 8; Abschnitt 1.4 von Anhang 1; Abschnitt 3.1 der Zusammenfassung der Folgenabschätzung.

([4]) Arbeitsdokument der Datenschutzgruppe „Artikel 29" zum Thema „Datenschutz und geistiges Eigentum", WP 104.

([5]) Entschließung des Europäischen Parlaments vom 10. April 2008 zur Kulturwirtschaft in Europa (2007/2153(INI)), Nummer 23.

35. Der EDSB ist der Auffassung, dass ein Gleichgewicht zwischen dem legitimen Ziel der Bekämpfung illegaler Inhalte und der Angemessenheit der Mittel gefunden werden muss. Er weist darauf hin, dass jede Überwachung von Telekommunikationsnetzen, sofern sie in spezifischen Fällen erforderlich ist, Sache der Strafverfolgungsbehörden sein sollte.

IV. **FAZIT**

36. Der EDSB befürwortet den Vorschlag für ein Mehrjahresprogramm zum Schutz von Kindern bei der Nutzung des Internets und anderer Kommunikationstechnologien. Er begrüßt, dass mit diesem Programm in erster Linie auf die Entwicklung neuer Technologien und die Ausarbeitung konkreter Aktionen abgestellt wird, mit denen die Wirksamkeit des Schutzes der Kinder verbessert werden soll.

37. Der EDSB weist darauf hin, dass der Schutz personenbezogener Daten eine Grundvoraussetzung für die Sicherheit von Kindern bei der Nutzung des Internets. Der Missbrauch personenbezogener Daten von Kindern muss verhindert werden, indem die Zielsetzungen des Programms und insbesondere Folgendes zum Tragen kommen:

— Sensibilisierung von Kindern und anderen Akteuren wie Eltern und Erziehern,

— Förderung der Entwicklung vorbildlicher Praxislösungen durch die Industrie,

— Förderung der Entwicklung technologischer Instrumente, bei denen der Schutz der Privatsphäre gewahrt bleibt,

— Förderung des Austausches bewährter Verfahren und praktischer Erfahrungen zwischen den einschlägigen Behörden, einschließlich Datenschutzbehörden.

38. Bei der Durchführung dieser Maßnahmen darf nicht übersehen werden, dass der Schutz des Kindes in einem Umfeld erfolgt, in dem die Rechte anderer beeinträchtigt werden könnten. Jede Initiative zur Erhebung, Sperrung oder Meldung von Daten sollte ausschließlich unter Achtung der Grundrechte aller Beteiligten und unter Einhaltung des Rechtsrahmens für den Datenschutz erfolgen. Der EDSB weist insbesondere darauf hin, dass die Überwachung von Telekommunikationsnetzen, sofern sie in spezifischen Fällen erforderlich ist, Aufgabe der Strafverfolgungsbehörden sein sollte.

39. Der EDSB stellt fest, dass dieses Programm einen allgemeinen Rahmen für weitere konkrete Maßnahmen darstellt. Nach seiner Auffassung sind einige Bemerkungen in dieser Stellungnahme ein erster Schritt und könnten auf praktischer Ebene weiterentwickelt werden, und zwar unter Bezugnahme auf die noch auf den Weg zu bringenden Projekte im Einklang mit den Zielsetzungen des Programms. Er empfiehlt, dass die Datenschutzbehörden eng eingebunden werden, wenn es um die Festlegung dieser praktischen Projekte geht. Er verweist ferner auf die Tätigkeit der Datenschutzgruppe „Artikel 29“ zu dieser Frage und insbesondere auf die gegenwärtige Arbeit der Gruppe zu Social-Networking-Websites ([1]).

Brüssel, den 23. Juni 2008

Peter HUSTINX

Europäischer Datenschutzbeauftragter

([1]) Siehe Arbeitspapier 1/2008 vom 18. Februar 2008 zum Schutz personenbezogener Daten von Kindern, WP 147, und für einen allgemeinen Überblick das Arbeitsprogramm 2008-2009 der Arbeitsgruppe unter anderem zu sozialen Online-Netzwerken, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm