ARTIKEL-29-Datenschutzgruppe

01611/06/DE
WP 126

Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation

Angenommen am

26. September 2006

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie, ferner auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

1. Hintergrund

Am 29. Juni 2006 nahm die Europäische Kommission ihre Mitteilung über die Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste an [SEK (2006) 816] [SEK (206) 817]. Darin erläutert die Kommission die Funktionsweise der fünf Richtlinien des Rechtsrahmens für elektronische Kommunikationsnetze und –dienste[1] und legt dar, inwiefern die mit dem Rechtsrahmen verfolgten Ziele erreicht wurden und wo Änderungsbedarf besteht.

Die Mitteilung wird durch ein Arbeitspapier der Kommissionsdienststellen [KOM (206) 334 endg.] ergänzt, in dem die vorgeschlagenen Änderungen umgesetzt werden. Auf die vielfältigen Alternativen, die vor der Erarbeitung der in der Mitteilung dargelegten Schlussfolgerungen erwogen wurden, wird in der Folgenabschätzung eingegangen. Die genannten Dokumente bilden die Grundlage der öffentlichen Konsultation über den künftigen Rechtsrahmen für die elektronische Kommunikation, zu der bis spätestens 27. Oktober 2006 Stellungnahmen erwartet werden.

Unter Berücksichtigung der eingegangenen Stellungnahmen wird die Kommission einen Legislativvorschlag zur Änderung des Rechtsrahmens ausarbeiten, den sie dem Europäischen Parlament und dem Rat vorlegen wird.

Gegenstand der Überprüfung ist auch die Datenschutzrichtlinie für elektronische Kommunikation, die zu den fünf Richtlinien über elektronische Kommunikationsnetze und –dienste gehört. Nachstehend findet sich der Beitrag der Artikel-29-Datenschutzgruppe zur öffentlichen Konsultation mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation:

2. Allgemeine Bemerkungen

Das Hauptaugenmerk der Artikel-29-Datenschutzgruppe gilt der Verarbeitung personenbezogener Daten über elektronische Kommunikationsnetze und ihrer Sicherheit, da hier eine Reihe von Datenschutzfragen berührt werden, die die Artikel-29-Datenschutzgruppe in dieser Stellungnahme behandeln möchte.

[1] Richtlinie 19/2002/EG, ABl. L 108 vom 24.4.2002, S.7; Richtlinie 20/2002/EG, ABl. L 108 vom 24.4.2002, S. 21; 21/2002/EG, ABl. L 108 vom 24.4.2002, S. 33; Richtlinie 22/2002/EG, ABl. L 108 vom 24.4.2002, S. 51; Richtlinie 58/2002/EG, ABl. L 201 vom 31.7.2002, S. 37.

Bei der Evaluierung der Mitteilung mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation und etwaiger vorzunehmender Änderungen nimmt die Artikel-29-Datenschutzgruppe Bezug auf ihre Stellungnahme 7/200 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[2]. Da einigen darin enthaltenen Vorschlägen nicht Rechnung getragen wurde, möchte die Datenschutzgruppe sie erneut vorbringen.

1) Wie die Artikel-29-Datenschutzgruppe betonte, ist der Umstand, dass die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation nur für die Erbringung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen gelten, insofern bedauerlich, als private Netzwerke im täglichen Leben zunehmend an Bedeutung gewinnen und die Risiken entsprechend zunehmen, vor allem, weil derartige Netze immer spezifischer werden und z. B. zur Überwachung des Verhaltens von Angestellten mit Hilfe von Verkehrsdaten eingesetzt werden. Eine Überprüfung des Geltungsbereichs der Richtlinie ist auch deswegen geboten, weil sich private und öffentliche Dienste zunehmend vermischen.

2) Die Definitionen der Begriffe „elektronische Kommunikationsdienste“ und „Bereitstellung eines elektronischen Kommunikationsnetzes“ sind noch nicht eindeutig und beide Begriffe sollten näher erläutert werden, um sowohl den für die Datenverarbeitung Verantwortlichen als auch den Nutzern eine klare und eindeutige Auslegung zu ermöglichen. Die unklaren Definitionen werfen verschiedene Fragen auf, zum Beispiel: „Ist ein Internetcafe als Bereitsteller eines elektronischen Kommunikationsnetzes zu betrachten“? Derartige Fragen sollten einfach zu beantworten sein, doch dies nicht immer der Fall.

3) Darüber hinaus nahm die Artikel-29-Datenschutzgruppe in ihrer vorhergehenden Stellungnahme 7/2000 hinsichtlich der Verwendung von Cookies auf Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation Bezug. Erwägungsgrund 25 ist zu entnehmen, dass die Nutzer die Gelegenheit haben sollten, die Speicherung eines Cookies in ihrem Endgerät abzulehnen. Die Artikel-29-Datenschutzgruppe unterstützt diesen Standpunkt uneingeschränkt. Im letzten Absatz dieses Erwägungsgrunds 25 heißt es, dass der Zugriff auf spezifische Website-Inhalte davon abhängig gemacht werden kann, dass ein Cookie akzeptiert wird. Dies könnte dem Standpunkt zuwiderlaufen, wonach die Nutzer die Gelegenheit haben sollten, die Speicherung eines Cookies in ihren Endgeräten abzulehnen. Daher bedarf dieser Absatz gegebenenfalls einer Klärung oder Änderung.

3. Besondere Anmerkungen zu einzelnen Absätzen

Arbeitspapier der Kommissionsdienststellen, Abschnitt 5.8: Verbesserung der Durchsetzungsverfahren unter dem Rechtsrahmen

Gegenstand dieses Abschnitts ist die Notwendigkeit einer Anpassung der Durchsetzungsverfahren und –befugnisse, die den Behörden, welche die Datenschutzrichtlinie für elektronische Kommunikation umsetzen, zur Verfügung stehen.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf

Wie festgestellt wird, haben sich Geldstrafen für die Nichteinhaltung der Rechtsvorschriften als nicht sinnvoll erwiesen, denn die bei Verletzung der Datenschutzrichtlinie für elektronische Kommunikation vorgesehenen Geldstrafen seien zu niedrig, und ihre Anwendung zu uneinheitlich.

Möglicherweise sind die bei der Durchsetzung beobachteten Unterschiede nicht durch die Datenschutzrichtlinie für elektronische Kommunikation, sondern durch Unterschiede bei der Umsetzung in innerstaatliches Recht bedingt. So gibt es in den Mitgliedstaaten zum Beispiel verschiedene Auslegungen von Artikel 13 Absatz 2 sowie unterschiedliche Höchststrafen bei Verletzung dieser Richtlinie.

Höhere und einheitliche Strafen mögen zwar ein effizienteres Abschreckungsmittel sein, doch können sie die beobachtete uneinheitliche Durchsetzung vermutlich nicht allein ausräumen. Darüber hinaus sind die möglichen Strafen nicht unbedingt ausschlaggebend dafür, mit welcher Häufigkeit die Durchsetzungsbefugnisse ausgeübt werden. Die Art dieser Befugnisse und die Verfahren für ihre Ausübung sind möglicherweise wichtigere Faktoren.

In einigen Mitgliedstaaten verfügen die Datenschutzbehörden der Mitgliedstaaten nur über beschränkte Ermittlungsbefugnisse, die ihnen zum Beispiel keinen Zugriff auf die Kommunikationsdaten ermöglichen, die zum Nachweis eines Verstoßes gegen die Richtlinie erforderlich sind.

Wenn die Gesetzgeber in mehreren Mitgliedstaaten angesichts der derzeitigen Durchsetzungsbefugnisse nicht in der Lage sind, rasch zu handeln, muss etwas dagegen unternommen werden. Eine weitere Schwierigkeit bei der Durchführung besteht darin, dass viele Spammer nicht in den Zuständigkeitsbereich von Behörden in der EU fallen. Dieses Problem sollte durch eine enge Zusammenarbeit mit den Aufsichtsbehörden anderer Länder gelöst werden.

Was das im Arbeitspapier der Kommissionsdienststellen genannte explizite Recht auf ein Vorgehen gegen Spammer betrifft, ist nicht klar, was sich dadurch gegenüber der derzeitigen Situation ändern würde, bei der die zuständige Behörde Durchsetzungsmaßnahmen gegen alle treffen kann, die gegen die geltende Richtlinie verstoßen.

Arbeitspapier der Kommissionsdienststellen, Abschnitt 7: Sicherheit

In diesem Abschnitt wird im Wesentlichen vorgeschlagen, die Sicherheitsbestimmungen auszuweiten und zu verstärken. Die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation sollen mit denen der Universaldienstrichtlinie zusammengefasst werden in einem eigenen Kapitel der Rahmenrichtlinie, das Sicherheitsbestimmungen zum Gegenstand hat.

Die Stärkung der Sicherheitsbestimmungen dürfte den Datenschutzinteressen der Verbraucher zugute kommen, doch bleibt unklar, inwiefern die Verfassung eines eigenen gemischten Kapitels nützlich sein könnte. Es könnte argumentiert werden, dass eine Streichung der Sicherheitsbestimmungen aus der Datenschutzrichtlinie für elektronische Kommunikation nicht - wie im Arbeitsdokument der Kommissionsdienststellen dargelegt - die Bedeutung des Themas herausstellen, sondern vielmehr der Eindruck vermittelt würde, dass die Sicherheit nur die Netzwerke, den Wettbewerb und die Netzbetreiber betrifft. Ganz im Gegenteil betrifft sie jedoch auch den Schutz des Grundrechts auf Datenschutz, wie in der Datenschutzrichtlinie für elektronische Kommunikation ausgeführt.

Die Artikel-29-Datenschutzgruppe möchte hinzufügen, dass nicht die „Sicherheit“ im weitesten Sinne, sondern bestimmte Sicherheitsaspekte behandelt werden sollten. Aufmerksamkeit sollte nicht nur der „Kontinuität“ und „Vertraulichkeit“, sondern auch der „Integrität“ der Daten und insbesondere Fragen, die mit dem Aspekt Authentifizierung versus Anonymität zusammenhängen, geschenkt werden. Da ein Mangel an geeigneten Authentifizierungsverfahren zur Entstehung von Betrugsmustern führen und das Vertrauen der Nutzer in die elektronische Kommunikation beeinträchtigen könnte, wäre zu erwägen, in die Einführung zu Kapitel 7 einen Unterabschnitt zum Thema „Identitätsbetrug“ aufzunehmen. In diesem Unterabschnitt könnte ausgeführt werden, dass sowohl die Vertraulichkeit als auch das zeitgerechte Löschen eines Übermaßes an persönlichen Daten dazu beitragen, Identitätsdiebstahl vorzubeugen.

Bei der Behandlung der Authentifizierungsfragen ist jedoch zu berücksichtigen, dass Privatpersonen grundsätzlich in der Lage sein müssen, öffentliche elektronische Dienste anonym zu nutzen. Daher muss vor einem Vorschlag oder einer Änderung im Bereich der Authentifizierung der Zugang zu elektronischen Diensten umfassend analysiert werden, denn eine freie Kommunikation ist sehr wichtig. Dabei könnte sich zeigen, dass verschiedenen Betrugsarten dadurch zu begegnen ist, dass die Diensteanbieter eine Authentifizierung verlangen. Diesbezügliche Arbeiten wären zu begrüßen.

Arbeitspapier der Kommissionsdienststellen, Abschnitt 7.1: Verpflichtung, Sicherheitsmaßnahmen zu ergreifen, und Befugnisse der Nationalen Aufsichtsbehörden im Bereich der Festlegung und Überwachung der technischen Umsetzung

In diesem Abschnitt wird die Ansicht vertreten, dass der vorliegende Rahmen den Diensteanbietern bei der Bewertung ihrer eigenen Sicherheitsmaßnahmen zu viel Spielraum lässt. Angesichts der zunehmenden Sicherheitsbedrohungen bedürfe es zwecks Erhöhung der Effizienz der Sicherheitsmaßnahmen einer Klärung der in Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation verwendeten Begriffe.

Dazu wären neue Verpflichtungen vorzusehen, wie: Maßnahmen zur Behandlung sicherheitsrelevanter Ereignisse; die Vorschrift, die Leitlinien der Aufsichtsbehörden zu befolgen; Vertragsbestimmungen, die die Verbraucher darüber informieren, welche Maßnahmen bei Sicherheitsverstößen getroffen werden.

Erstens ist unklar, inwieweit diese Vorschläge zum vorhandenen Rahmen beitragen können – außer der Tatsache, dass festgeschrieben wird, was die meisten Aufsichtsbehörden bereits voraussetzen würden. So wird wahrscheinlich keine Aufsichtsbehörde meinen, dass ein Diensteanbieter, dessen Sicherheitsmaßnahmen keine Verfahren für den Umgang mit sicherheitsrelevanten Vorfällen und die Minimierung der Auswirkungen auf die Verbraucher umfassen, den Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation genügt.

Zweitens dürfte die Frage, ob ein Diensteanbieter die Leitlinien der Aufsichtsbehörde missachtet, auch heute bereits in gewisser Weise darüber entscheiden, ob der Diensteanbieter gegen Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation verstößt. Daher ist nur schwer erkennbar, inwiefern mit der Verpflichtung der Anbieter, derartige Leitlinien zu befolgen, mehr erreicht werden könnte, als wenn die Aufsichtsbehörden die geltenden Bestimmungen sinnvoll anwenden.

Drittens ist nicht deutlich, ob vertragliche Bestimmungen, mit denen die Kunden darüber informiert werden, welche Maßnahmen sie im Falle von Sicherheitsverstößen ergreifen könnten, mehr als eine „kosmetische Übung“ sein können.

Bei der Einführung derartiger Bestimmungen besteht die Gefahr, dass durch die Reglementierung nicht nur für den Sektor, sondern auch für die Aufsichtsbehörden die Belastung zunimmt. Der Sektor ist so beschaffen, dass den Datenschutzbehörden nicht möglich ist, Sicherheitsbestimmungen in Form verbindlicher Anweisungen festzulegen. Die Maßnahmen müssen sektorspezifischer Art sein, und sie ändern sich zu rasch, als dass eine Behörde den gesamten Sektor überwachen könnte; außerdem gibt es natürlich eine Vielzahl spezialisierter Sicherheitsexperten, die besser in Sicherheitsfragen beratend tätig werden und Prüfungen vornehmen können.

Klarstellungen und verbindliche Anweisungen sollten von einer sektorspezifischen Behörde und nicht von Datenschutzexperten kommen. Auch gilt es, schwerfällige Regelungen zu vermeiden, denn, wie im Arbeitsdokument der Kommissionsdienststellen (Fußnote 30) festgestellt wird, muss bei der Behandlung von Sicherheitsfragen über die Regelungen hinausgegangen werden.

Arbeitspapier der Kommissionsdienststellen, Abschnitt 7.2: Meldung von Sicherheitsverstößen durch Netzbetreiber und Diensteanbieter

Deshalb begrüßt die Artikel-29-Datenschutzgruppe den Vorschlag, die Meldung von Sicherheitsverstößen vorzuschreiben; die Kommission plant jedoch keine Sanktion für den Fall, dass ein Netzbetreiber oder Diensteanbieter die Nationale Aufsichtsbehörde nicht informiert.

Die Artikel-29-Datenschutzgruppe erwartet Einwände des Sektors in dem Sinne, dass hier eine Art Sonderbehandlung eingeführt wird, für andere Sektoren hingegen keine Meldepflicht besteht. Die Artikel-29-Datenschutzgruppe räumt ein, dass derartige Vorschriften derzeit ein aktuelles Thema sind, und wichtiger noch, dass dies eine „vereinfachte“ Regelung darstellt, die Diensteanbieter, welche angemessene Maßnahmen durchführen, nur wenig mehr belastet, jedoch ein echtes marktgesteuertes Abschreckungsmittel für diejenigen bildet, die Vorschriften umgehen wollen.

Auf der anderen Seite ist festzustellen, dass keiner der in letzter Zeit aus den USA gemeldeten Sicherheitsverstöße (Choicepoint, LexisNexis, Bank of America, Time Warner usw.) Diensteanbieter betraf. Die Artikel-29-Datenschutzgruppe schlägt vor, dass die Meldepflicht auch für „Datenmakler“, Banken und andere Anbieter von Onlinediensten in Betracht gezogen werden sollte. Sie mögen zwar keine Anbieter von Internetdiensten sein, doch sind sie von Sicherheitsverstößen am meisten betroffen.

Gemäß dem Vorschlag soll der Diensteanbieter nur das Opfer seiner Kunden über einen Sicherheitsverstoß informieren. Bei schwerwiegenden Verstößen (mit der Mitteilung soll keine Einteilung der Verstöße in Schweregrade vorgenommen oder festgelegt werden, wann ein Verstoß der Meldepflicht unterliegt) müssen jedoch alle Kunden des Diensteanbieters und nicht nur die „Opfer“ informiert werden. Der Legislativvorschlag müsste Regeln für eine Einteilung der Verstöße in Schweregrade festlegen.

Zugangsanbieter und Diensteanbieter

In der Mitteilung wird zwischen Zugangsanbietern und Diensteanbietern unterschieden. In Artikel 3 der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation ist festgelegt, auf welche Form von Datenverarbeitung sich die Bestimmungen beziehen. Während früher klar war, wer als Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste zu betrachten war, wird es aufgrund von Entwicklungen auf dem Gebiet der elektronischen Kommunikation für die Verbraucher möglicherweise schwieriger, festzustellen, wer einen Dienst tatsächlich erbringt. So kann es vorkommen, dass die Verbraucher über ein Portal auf einen Dienst zugreifen, der von verschiedene Parteien angeboten wird.

Wenn es um Aspekte wie die Bereitstellung von Informationen und die Erteilung des Einverständnisses geht, ist vielleicht nicht immer klar, wer dafür zuständig ist, die Nutzer zu informieren oder wem das Einverständnis zu erteilen ist. Gleichzeitig könnten Diensteanbieter Nutzer irrtümlicherweise zu einem Zugangs- oder Netzanbieter umleiten, der sich um spezielle technische Aspekte des Dienstes kümmert.

Angesichts der besonderen Rollen, die Zugangsanbieter und Diensteanbieter haben können, ist es möglicherweise sinnvoll zu untersuchen, ob die Vorschriften über die Verarbeitung persönlicher Daten und den Datenschutz im elektronischen Kommunikationssektor verschärft werden müssen, um jegliches Missverständnis über die Frage, auf wen die Bestimmungen abzielen, zu vermeiden. Daher sollte der Legislativvorschlag eine Klärung und keine zusätzliche Verwirrung bewirken.

4. Schlussfolgerung

Die Artikel-29-Datenschutzgruppe begrüßte die Gelegenheit zur Überprüfung der fünf Richtlinien über elektronische Kommunikation mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation Stellung zu nehmen. Die Artikel-29-Datenschutzgruppe empfiehlt zunächst eine Verstärkung der Sicherheitsmaßnahmen und betont, dass neben der Verbesserung der Sicherheit der Infrastruktur auch dem Schutz der Nutzer und der Förderung ihres Vertrauens in die elektronische Kommunikation umfassend Rechnung getragen werden sollte.

Die Artikel-29-Datenschutzgruppe schlägt des Weiteren die Behandlung der mit Onlineanwendungen verbundenen Themen vor. Dazu zählen Sicherheitsfragen, die Verantwortung der Betreiber sowie die Klärung des rechtlichen Status und der Definition des für die Datenverarbeitung Verantwortlichen.

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass sie zwar die Verbesserung der Sicherheitsmaßnahmen unterstützt, spricht sich aber gegen alle Maßnahmen aus, die zu einer verstärkten Überwachung oder Sperrung von Inhalten führen oder führen könnten.

Die Datenschutzgruppe behält sich vor, die kommenden Fassungen der Richtlinie zu kommentieren.

Brüssel, den 26. September 2006

Für die Datenschutzgruppe

Der Vizepräsident
Jose Luis Piñar Mañas