

675.32.30

Gemeinsamer Standpunkt zu Datenschutz bei Suchmaschinen im Internet

- zuerst verabschiedet auf der 23. Sitzung in Hong Kong SAR, China, 15. April 1998 -
- überarbeitet und aktualisiert auf der 39. Sitzung, 6.-7. April 2006, Washington, D.C. (USA) -

- Übersetzung -

Gegenwärtig enthält das Internet eine riesige Menge an Informationen über fast jeden Sachverhalt, den man sich vorstellen kann. Zum Auffinden der gewünschten Information im Internet sind Suchmaschinen zu einem unverzichtbaren Werkzeug geworden. Sie sind die Schlüssel zum „cyber-space“.

Mit diesen Suchmaschinen kann man nach veröffentlichten personenbezogenen Daten suchen. Als Ergebnis erhält man ein Profil der Aktivitäten einer bestimmten Person im Internet. Suchmaschinen können auch für das „data-mining“ genutzt werden. Da das Internet für den Austausch von Informationen und andere Aktivitäten (z. B. den elektronischen Geschäftsverkehr) immer populärer wird, kann dies zu einer Gefährdung der Privatsphäre führen.

Darüber hinaus können Betreiber von Suchmaschinen detaillierte Profile der Interessen ihrer Nutzer erstellen. IP-Protokolldaten ermöglichen die Identifizierung von Nutzern, insbesondere dann, wenn sie mit entsprechenden bei Zugangsdiensteanbietern gespeicherten Daten kombiniert werden. Da die Nutzung von Suchmaschinen heutzutage eine gängige Praxis unter Nutzern des Internet darstellt, ermöglichen bei den Betreibern populärer Suchmaschinen gespeicherte Verkehrsdaten detaillierte Profile über Interessen, Meinungen und Aktivitäten über verschiedene Bereiche hinweg (z.B. Beruf, Freizeit, politische Meinungen, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit besonders besorgt über die Möglichkeit gezeigt, Persönlichkeitsprofile von Bürgern zu erstellen. Dies ist jetzt in einem gewissen Maß auf globaler Ebene durch die im Internet zur Verfügung gestellte Technologie möglich geworden.

Die Arbeitsgruppe hat bereits in der Vergangenheit Probleme des Datenschutzes und der Privatsphäre im Zusammenhang mit der Nutzung des Internet betont und Empfehlungen zu möglichen Schritten zur Lösung dieser Probleme gegeben. Im Hinblick auf übermittelte oder veröffentlichte personenbezogene Daten erinnert die Arbeitsgruppe daran, dass auch personenbezogene Daten, die der Nutzer freiwillig veröffentlicht hat, auch dann noch den für sie geltenden Schutzbestimmungen unterliegen.

Empfehlungen

Secretariat
Berliner Datenschutzbeauftragter
Pallasstr 25/26
D-10781 Berlin
Phone +49 / 30 / 7876 8844
Fax: +49 / 30 / 216 9927

E-Mail:
mailto:mailbox@datenschutz-berlin.de

Internet:
<http://www.datenschutz-berlin.de>

The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

Nutzer des Internets können gleichzeitig auch Informationsanbieter sein. Sie sollten sich darüber im klaren sein, daß jedes personenbezogene Datum, das sie im Netz publizieren (z. B. bei der Einrichtung ihrer eigenen Homepage, oder bei der Veröffentlichung von Artikeln in newsgroups), von Dritten für die Erstellung eines Profils genutzt werden kann.

So können zum Beispiel Nachrichten in newsgroups oder bei „social networking“ Angeboten von Suchmaschinen durchsucht und indexiert werden, und damit zur Anreicherung von Profilen darüber beitragen, wer sich zu welchem Thema wie geäußert hat. Eine Möglichkeit, diese Gefährdung für die Privatsphäre zu reduzieren kann zum Beispiel bei der Teilnahme an newsgroups in der Nutzung von Pseudonymen bestehen.

Daher sollten Diensteanbieter und Softwarehersteller im Internet ihren Nutzern die Nutzung ihrer Dienste unter Pseudonym anbieten. Jedenfalls sollten die Nutzer auf das Risiko aufmerksam gemacht werden, das sie eingehen, wenn sie an News-Diensten, chat-Räumen oder „social networking“-Angeboten unter ihrer echten E-mail-Adresse oder sogar ihrem wirklichen Namen teilnehmen.

Die Nutzer sollten die Möglichkeit haben, die Nutzung ihrer Daten auf bestimmte Zwecke zu beschränken. Sie sollten darüber hinaus in die Lage versetzt werden, ihre eigenen Informationen im Netz (oder Teile davon) gegen die Überwachung durch Suchmaschinen zu schützen. Dies kann zum Beispiel durch das Setzen einer „no-robots“-Option für eine Website erreicht werden. Allerdings setzt die Wirksamkeit dieser Einrichtung voraus, daß sie von den Anbietern von Suchmaschinen beachtet wird.

Anbieter von Suchmaschinen sollten die Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung ihrer Dienste informieren.

Sie sollten darüber hinaus den Betroffenen ein Mittel zur Verfügung stellen, um ihre Daten aus (veralteten) möglicherweise bei den Anbietern gespeicherten Kopien von Seiten löschen zu lassen („cache“).

Im Hinblick auf die Sensibilität der Spuren, die Betroffene bei der Nutzung von Suchmaschinen hinterlassen, sollten Betreiber von Suchmaschinen ihre Dienste in datenschutzfreundlicher Weise anbieten. Insbesondere sollten sie keine Informationen über Suchvorgänge, die mit einzelnen Nutzern in Verbindung gebracht werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende einer Suchmaschinen-Sitzung sollten keine Daten gespeichert bleiben, die mit einem einzelnen Nutzer in Verbindung gebracht werden können, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung zur Speicherung von zur Erbringung eines Dienstes erforderlichen Daten gegeben.

Der Minimierung von Daten kommt in jedem Fall eine Schlüsselposition zu. Eine solche Praxis wäre auch im Interesse der Anbieter von Suchmaschinen, die zunehmend mit Forderungen Dritter nach nutzerspezifischen Informationen umgehen müssen.

Zum Schutz der Privatsphäre der Benutzer ist der umfassende Einsatz von datenschutzfreundlichen Technologien erforderlich, wo dies möglich ist.