



00737/DE
WP 148

**Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit
Suchmaschinen**

Angenommen am 4. April 2008

Diese Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro LX-46 06/80.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

Inhaltsverzeichnis

ZUSAMMENFASSUNG	3
1. EINLEITUNG	4
2. DEFINITION FÜR „SUCHMASCHINE“ UND GESCHÄFTSMODELL	6
3. UM WELCHE ARTEN VON DATEN GEHT ES?	6
4. RECHTSRAHMEN	8
4.1. Verantwortliche für die Verarbeitung von Benutzerdaten	8
4.1.1. Das Grundrecht – Achtung der Privatsphäre.....	8
4.1.2. Anwendbarkeit der Richtlinie 95/46/EG (Datenschutzrichtlinie).....	9
4.1.3 Anwendbarkeit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten).....	13
4.2 Anbieter von Inhalten	14
4.2.1. Freie Meinungsäußerung und Recht auf Privatsphäre.....	14
4.2.2 Datenschutzrichtlinie	15
5. RECHTMÄSSIGKEIT DER VERARBEITUNG.....	17
5.1. Von den Suchmaschinenbetreibern vorgebrachte Zwecke und Gründe.....	17
5.2. Analyse der Zwecke und Gründe durch die Arbeitsgruppe	18
5.3. Von der Branche zu klärende Fragen	21
6. VERPFLICHTUNG ZUR INFORMATION DER BETROFFENEN PERSON.....	25
7. RECHTE DER BETROFFENEN PERSON	26
8. SCHLUSSFOLGERUNGEN	27
ANHANG 1 BEISPIELE FÜR DIE VON SUCHMASCHINEN VERARBEITETEN DATEN UND TERMINOLOGIE.....	31
ANHANG 2.....	33

ZUSAMMENFASSUNG

Suchmaschinen sind zu einem festen Bestandteil des Alltags der Menschen geworden, die das Internet und Technologien zur Informationsgewinnung nutzen. Die Artikel-29-Datenschutzgruppe ist sich der Nützlichkeit von Suchmaschinen bewusst und erkennt ihre Bedeutung an.

In der vorliegenden Stellungnahme benennt die Arbeitsgruppe klare Verantwortlichkeiten im Rahmen der Datenschutzrichtlinie (95/46/EG) für Suchmaschinenbetreiber in ihrer Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten. In bestimmten Situationen ist das europäische Datenschutzrecht auch auf Suchmaschinen anwendbar, wenn sie als Anbieter von Inhaltsdaten (d. h. Index der Suchergebnisse) fungieren, z. B. wenn sie einen Caching-Dienst anbieten oder sich auf die Erstellung von Personenprofilen spezialisieren. Vorrangiges Ziel dieser Stellungnahme ist es, ein Gleichgewicht zwischen den berechtigten geschäftlichen Erfordernissen der Suchmaschinenbetreiber und dem Schutz der personenbezogenen Daten von Internet-Benutzern herzustellen.

Diese Stellungnahme befasst sich mit der Definition von Suchmaschinen, den Arten der bei der Bereitstellung von Suchdiensten verarbeiteten Daten, dem Rechtsrahmen, den Zwecken/Gründen für eine zulässige Verarbeitung, der Verpflichtung zur Information der betroffenen Personen und den Rechten der betroffenen Personen.

Eine wichtige Schlussfolgerung dieser Stellungnahme besteht darin, dass die Datenschutzrichtlinie grundsätzlich auf die Verarbeitung personenbezogener Daten durch Suchmaschinen anwendbar ist, auch wenn sich deren Hauptsitz außerhalb des EWR befindet, und dass es unter diesen Umständen Sache der Suchmaschinenbetreiber ist, ihre Rolle im EWR und den Umfang ihrer Verantwortlichkeiten im Rahmen der Richtlinie zu klären. Des Weiteren wird klargestellt, dass die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) eindeutig nicht auf Suchmaschinenbetreiber anwendbar ist.

Die vorliegende Stellungnahme kommt zu dem Ergebnis, dass personenbezogene Daten nur für rechtmäßige Zwecke verarbeitet werden dürfen. Die Suchmaschinenbetreiber müssen personenbezogene Daten löschen oder irreversibel anonymisieren, sobald sie der angegebenen rechtmäßigen Zweckbestimmung nicht mehr dienen, und sie müssen in der Lage sein, die Speicherung und die Lebensdauer der gesetzten Cookies jederzeit zu begründen. Bei allen geplanten Querverbindungen von Benutzerdaten und bei der Anreicherung von Benutzerprofilen muss die Einwilligung des Benutzers eingeholt werden. Die Suchmaschinen müssen Nichtbeteiligungsklauseln („Opt-outs“) von Website-Herausgebern beachten und den Aufforderungen von Benutzern zur Aktualisierung oder Auffrischung ihrer Cache-Speicher unverzüglich nachkommen. Die Arbeitsgruppe erinnert in diesem Zusammenhang an die Verpflichtung der Suchmaschinen, die Benutzer im Vorhinein über alle beabsichtigten Verwendungszwecke ihrer Daten zu informieren und ihre Rechte auf Auskunft, Einsichtnahme oder Berichtigung ihrer personenbezogenen Daten gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zu respektieren.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995¹,

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

gestützt auf Artikel 255 EG-Vertrag und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

Die Suchmaschinenbetreiber im World Wide Web erfüllen als Vermittler eine überaus wichtige Rolle in der Informationsgesellschaft. Die Arbeitsgruppe erkennt die Notwendigkeit und die Nützlichkeit von Suchmaschinen an und ist sich ihres Beitrags zur Entwicklung der Informationsgesellschaft bewusst.

Für die unabhängigen Datenschutzbehörden im EWR spiegelt sich die wachsende Bedeutung der Suchmaschinen aus Datenschutzsicht in der steigenden Zahl der Beschwerden von Personen („betroffene Personen“) über mögliche Verstöße gegen ihr Recht auf Privatsphäre wider. Zudem ist die Zahl der Anfragen seitens der für die Verarbeitung Verantwortlichen sowie seitens der Presse bezüglich der Auswirkungen von Internet-Suchdiensten auf den Schutz personenbezogener Daten spürbar gestiegen.

In den Beschwerden der betroffenen Personen spiegeln sich ebenso wie in den Anfragen der für die Verarbeitung Verantwortlichen und der Presse die zwei verschiedenen Rollen wider, die Suchmaschinenbetreiber in Bezug auf personenbezogene Daten spielen.

Erstens erheben und verarbeiten Suchmaschinenbetreiber in ihrer Rolle als Diensteanbieter gewaltige Mengen an Benutzerdaten, darunter auch Daten, die mit technischen Mitteln wie Cookies erfasst werden. Das Spektrum der erhobenen Daten kann von den IP-Adressen einzelner Benutzer bis hin zu umfangreichen Suchhistorien sowie Daten reichen, die bei der Anmeldung für die Nutzung personalisierter Dienste von den Benutzern selbst eingegeben wurden. Die Erhebung von Benutzerdaten wirft zahlreiche Fragen auf. Durch den Fall AOL wurde einem breiten Publikum die Sensibilität von personenbezogenen Daten, die in Suchprotokollen enthalten sind, deutlich vor Augen geführt.² Nach Auffassung der Arbeitsgruppe haben die

¹ ABl. L 281 vom 23.11.1995, S. 31,

http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

² Im Sommer 2006 veröffentlichte AOL eine Liste der Suchanfragen, die von rund 650 000 Benutzern über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben worden waren. Obwohl

Suchmaschinenbetreiber in ihrer Rolle als Sammler von Benutzerdaten die Benutzer ihrer Dienste bisher noch nicht ausreichend über die Art und den Zweck ihrer Tätigkeit informiert.

Zweitens tragen Suchmaschinenbetreiber in ihrer Rolle als Anbieter von Inhalten dazu bei, dass ein weltweites Publikum einfachen Zugriff auf Veröffentlichungen im Internet erhält. Einige Suchmaschinen veröffentlichen Daten in einem so genannten „Cache“ (Zwischenspeicher) erneut. Durch die Wiedergewinnung und Zusammenfassung verschiedener Arten von Informationen über eine einzelne Person können Suchmaschinen ein neues Bild entstehen lassen, das mit wesentlich höheren Risiken für die betroffene Person behaftet ist, als wenn jedes in das Internet eingestellte Datenelement für sich isoliert bleiben würde. Die Darstellungs- und Aggregierungsfunktionen von Suchmaschinen können weit reichende Folgen für die Menschen sowohl in ihrem Privatleben als auch in der Gesellschaft haben. Das gilt vor allem, wenn die personenbezogenen Daten in den Suchergebnissen unrichtig, unvollständig oder überzogen sind.

Am 15. April 1998 hat die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (International Working Group on Data Protection in Telecommunications – IWGDPT)³ einen Gemeinsamen Standpunkt zu Datenschutz bei Suchmaschinen im Internet angenommen, der am 6./7. April 2006 überarbeitet wurde.⁴ Die Arbeitsgruppe zeigte sich darin besorgt über die Möglichkeit von Suchmaschinenbetreibern, Profile von natürlichen Personen erstellen zu lassen. In diesem Gemeinsamen Standpunkt wurde ausgeführt, wie bestimmte Aktivitäten von Suchmaschinenbetreibern die Privatsphäre der Bürger bedrohen können und dass personenbezogene Daten jeglicher Art, die auf einer Website eingestellt werden, von Dritten zur Erstellung von Personenprofilen verwendet werden könnten.

Außerdem wurde auf der 28. Internationalen Konferenz der Datenschutzbeauftragten am 2./3. November 2006 in London die EntschlieÙung zum Datenschutz bei Suchmaschinen (Resolution on Privacy Protection and Search Engines)⁵ angenommen. In der EntschlieÙung werden die Betreiber von Suchmaschinen aufgefordert, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Strategiepapieren und Verträgen niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern. Darüber hinaus werden in der EntschlieÙung verschiedene Aspekte im Zusammenhang mit Server-Protokollen, kombinierten Suchanfragen und deren Speicherung und der Erstellung detaillierter Profile von Benutzern erörtert.

AOL die Namen der Benutzer durch eine Zahl ersetzt hatte, fanden Journalisten heraus, dass die Ergebnisse der Suchanfragen oftmals zu den einzelnen Benutzern zurückverfolgt werden konnten, nicht nur wegen so genannter „Eitelkeitsanfragen“ (Suche mit eigenem Namen als Suchbegriff nach sich selbst), sondern auch aufgrund des Inhalts ihrer kombinierten Suchanfragen.

³ Die Arbeitsgruppe wurde auf Betreiben der Datenschutzbeauftragten verschiedener Länder gebildet, um die Privatsphäre und den Datenschutz in der Telekommunikation und in den Medien zu verbessern.

⁴ <http://www.datenschutz-berlin.de/attachments/44/Dokumente1998.pdf?1164728350>

⁵ <http://www.privacyconference2006.co.uk/index.asp?PageID=3>

2. DEFINITION FÜR „SUCHMASCHINE“ UND GESCHÄFTSMODELL

Generell sind unter Suchmaschinen Dienste zu verstehen, die ihren Benutzern beim Auffinden von Informationen im Internet helfen. Suchmaschinen können nach der Art der abzurufenden Daten unterschieden werden, darunter Bilder und/oder Videos und/oder Audiodaten oder verschiedene Arten von Formaten. Ein neues Entwicklungsgebiet sind Suchmaschinen, die sich auf die Erstellung von Personenprofilen auf Basis von personenbezogenen Daten spezialisiert haben, die irgendwo im Internet gefunden wurden. Im Rahmen der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) werden Suchmaschinen als Dienste der Informationsgesellschaft⁶ bezeichnet, d. h. als Instrumente zur Lokalisierung von Informationen⁷. Die Arbeitsgruppe verwendet diese Einstufung als Ausgangspunkt.

Die Arbeitsgruppe konzentriert sich in dieser Stellungnahme hauptsächlich auf Suchmaschinenbetreiber, die sich am vorherrschenden Geschäftsmodell für Suchmaschinen orientieren und sich durch Werbung finanzieren. In diese Kategorie fallen alle großen und bekannten Suchmaschinen, spezialisierte Suchmaschinen, die sich auf die Erstellung von Personenprofilen konzentrieren, sowie Meta-Suchmaschinen, die die Ergebnisse anderer Suchmaschinen präsentieren und eventuell neu zusammenfassen. Die Stellungnahme befasst sich nicht mit Suchfunktionen, die in Websites eingebettet sind und sich auf die Datensuche in der eigenen Domäne der Website beschränken.

Die Rentabilität derartiger Suchmaschinen hängt gewöhnlich von der Wirksamkeit der Werbung ab, die in Verbindung mit den Suchergebnissen angezeigt wird. Die Einnahmen werden überwiegend mit einem Pay-per-Click- (PPC) Verfahren erzielt. Bei diesem Geschäftsmodell berechnet die Suchmaschine dem Werbetreibenden einen bestimmten Betrag, sobald ein Benutzer auf einen gesponserten Link klickt. Die Untersuchung der Genauigkeit der Suchergebnisse und Werbeanzeigen konzentriert sich überwiegend auf die richtige Kontextualisierung. Damit die Suchmaschine die gewünschten Ergebnisse liefert und die Werbeanzeigen zur Optimierung der Einnahmen auch bei den richtigen Zielgruppen geschaltet werden, versuchen die Suchmaschinen möglichst viel über die Eigenschaften und den Kontext jeder einzelnen Suchanfrage herauszufinden.

3. UM WELCHE ARTEN VON DATEN GEHT ES?

Suchmaschinen verarbeiten eine große Vielfalt an Daten.⁸ Eine Liste der verschiedenen Arten von Daten findet sich im Anhang.

⁶ Internet-Suchmaschinen werden in den europäischen Rechtsvorschriften über die Dienste der Informationsgesellschaft behandelt, die in Artikel 2 der Richtlinie 2000/31/EG näher bezeichnet werden. Dieser Artikel verweist auf die Richtlinie 98/34/EG, die den Begriff „Dienst“ bzw. „Dienstleistung der Informationsgesellschaft“ spezifiziert.

⁷ Siehe Artikel 21 Absatz 2 in Verbindung mit dem Erwägungsgrund 18 der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG).

⁸ Die Artikel-29-Arbeitsgruppe hat unter anderem einen Fragebogen zur Datenschutzerklärung erstellt. Der Fragebogen wurde einer Reihe von Suchmaschinenbetreibern in den Mitgliedstaaten sowie verschiedenen Suchmaschinenbetreibern mit Sitz in den USA vorgelegt. Diese Stellungnahme beruht teilweise auf der Auswertung der Antworten auf diesen Fragebogen. Der Fragebogen ist in Anhang 2 dieser Stellungnahme beigefügt.

Protokolldateien

Die bei der Nutzung des Suchmaschinendienstes für den Benutzer angelegten Protokolldateien sind – sofern keine Anonymisierung erfolgt – die wichtigsten personenbezogenen Daten, die von den Suchmaschinenbetreibern verarbeitet werden. Die für die Nutzung des Dienstes typischen Daten lassen sich verschiedenen Kategorien zuordnen: Protokolle der Anfragen (Inhalt der Suchanfragen, Datum und Uhrzeit, Quelle (IP-Adresse und Cookie), benutzerspezifische Einstellungen und Daten, die sich auf den Computer des Benutzers beziehen); Daten über die angebotenen Inhalte (Links und Werbeanzeigen aufgrund jeder Anfrage) sowie Daten über die anschließende Benutzernavigation (Klicks). Die Suchmaschinen können auch operative Daten verarbeiten, die sich auf Benutzerdaten beziehen, Daten über registrierte Benutzer und Daten von anderen Diensten und aus anderen Quellen wie elektronische Post, Desktop-Suche und Werbeanzeigen auf Websites Dritter.

IP-Adressen

Ein Suchmaschinenbetreiber kann verschiedene Anfragen und Suchsitzungen, die von einer einzigen IP-Adresse ausgehen, miteinander verknüpfen.⁹ Daher können bei der Protokollierung der Suchvorgänge alle Suchvorgänge im Internet, die von einer bestimmten IP-Adresse ausgehen, verfolgt und korreliert werden. Die Identifizierung kann noch verbessert werden, wenn die IP-Adresse mit einem vom Suchmaschinenbetreiber übermittelten Cookie mit benutzerspezifischer Kennung korreliert wird, da sich dieses Cookie auch dann nicht ändert, wenn die IP-Adresse geändert wird.

Die IP-Adresse kann ebenfalls als Lokalisierungsinformation verwendet werden, auch wenn sie derzeit noch oftmals ungenau ist.

Web-Cookies

Benutzer-Cookies werden von der Suchmaschine übermittelt und auf dem Computer des Benutzers gespeichert. Der Inhalt der Cookies kann je nach Suchmaschinenbetreiber unterschiedlich sein. Die von Suchmaschinen gesetzten Cookies enthalten typischerweise Informationen über das Betriebssystem und den Browser des Benutzers sowie eine eindeutige Identifikationsnummer für jedes Benutzerkonto. Sie ermöglichen eine genauere Identifizierung des Benutzers als die IP-Adresse. Wenn beispielsweise mehrere Benutzer mit jeweils eigenem Konto denselben Computer benutzen, würde jeder Benutzer ein eigenes Cookie erhalten, der ihn als Benutzer des Computers eindeutig identifiziert. Wenn ein Computer eine dynamische und variable IP-Adresse besitzt und die Cookies am Ende einer Sitzung nicht gelöscht werden, kann mit einem derartigen Cookie der Benutzer von einer IP-Adresse zur nächsten verfolgt werden. Das Cookie kann auch zur Korrelation von Suchvorgängen verwendet werden, die von nomadischen Computern wie beispielsweise Laptops gestartet werden, da ein Benutzer an verschiedenen Orten dasselbe Cookie hätte. Wenn sich mehrere Computer einen Internet-Anschluss teilen (z. B. hinter einer Box oder einem Router mit Adressübersetzung der Absenderadresse (Network Address Translation – NAT), ermöglicht das Cookie die Identifizierung der einzelnen Benutzer an den verschiedenen Computern.

⁹ Immer mehr Internet-Diensteanbieter vergeben feste IP-Adressen an einzelne Benutzer.

Die Suchmaschinenbetreiber benutzen Cookies (gewöhnlich dauerhafte Cookies) zur Verbesserung der Qualität ihrer Dienstleistungen, indem sie die Benutzereinstellungen speichern und typische Merkmale des Benutzers, etwa sein Suchverhalten, verfolgen. Die meisten Browser sind standardmäßig so konfiguriert, dass sie Cookies akzeptieren. Der Browser kann aber auch so eingestellt werden, dass er alle Cookies ablehnt, nur Sitzungs-Cookies akzeptiert oder anzeigt, wann ein Cookie übermittelt wird. Eventuell funktionieren manche Merkmale und Dienste jedoch nicht richtig, wenn Cookies grundsätzlich abgelehnt werden, und zudem lassen sich erweiterte Funktionsmerkmale zur Cookie-Verwaltung nicht immer einfach konfigurieren.

Flash-Cookies

Einige Suchmaschinenbetreiber installieren Flash-Cookies auf dem Computer des Benutzers. Gegenwärtig können Flash-Cookies nicht ohne weiteres, etwa mit Hilfe der Standardlöschfunktionen der Internet-Browser, gelöscht werden. Bisher wurden Flash-Cookies unter anderem als Sicherung für normale Web-Cookies verwendet, die von den Benutzern leicht gelöscht werden können, oder auch zur Speicherung umfassender Informationen über Suchvorgänge der Benutzer (z. B. alle Internet-Anfragen, die an eine Suchmaschine übermittelt wurden).

4. RECHTSRAHMEN

4. 1. Verantwortliche für die Verarbeitung von Benutzerdaten

4.1.1. Das Grundrecht – Achtung der Privatsphäre

Im Hinblick auf die umfassende Erhebung und die Speicherung der Suchhistorien von Personen in direkt oder indirekt identifizierbarer Form kommt der Schutz personenbezogener Daten gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union zum Tragen.

Die Suchhistorie einer Person gibt Aufschluss über die Interessen, Beziehungen und Absichten dieser Person. Diese Daten können nachfolgend sowohl für kommerzielle Zwecke als auch – aufgrund von Anfragen und Phishing-Operationen und/oder Data Mining – von Strafverfolgungsbehörden oder nationalen Sicherheitsdiensten verwendet werden.

In Erwägungsgrund 2 der Richtlinie 95/46/EG heißt es: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und –freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.“

Die Suchmaschinen spielen eine entscheidende Rolle als erster Kontaktpunkt für den freien Zugriff auf Informationen im Internet. Dieser freie Zugriff auf Informationen ist für die persönliche Meinungsbildung in unserer Demokratie überaus wichtig. Aus diesem Grund ist Artikel 11 der Charta der Grundrechte der Europäischen Union von besonderer Bedeutung, da er vorsieht, dass Informationen ohne behördliche Eingriffe als Teil der Meinungsäußerung und Informationsfreiheit zugänglich sein sollten.

4.1.2. Anwendbarkeit der Richtlinie 95/46/EG (Datenschutzrichtlinie)

Die Artikel-29-Arbeitsgruppe hat sich bereits in ihren früheren Arbeitspapieren zu den Datenschutzbestimmungen aufgrund der Protokollierung von IP-Adressen und der Verwendung von Cookies im Rahmen der Dienste der Informationsgesellschaft geäußert. Die vorliegende Stellungnahme enthält weitere Leitlinien für die Anwendung der Definitionen von „personenbezogenen Daten“ und „für die Verarbeitung Verantwortlicher“ durch Suchmaschinenbetreiber. Suchmaschinendienste können im Internet innerhalb der EU bzw. des EWR, von einem Standort außerhalb des Hoheitsgebiets der EU/EWR-Mitgliedstaaten oder von mehreren Standorten in der EU bzw. im EWR und im Ausland bereitgestellt werden. Daher werden die Bestimmungen von Artikel 4 ebenfalls erörtert. Artikel 4 der Datenschutzrichtlinie befasst sich mit der Anwendbarkeit des einzelstaatlichen Datenschutzrechts.

Personenbezogene Daten: IP-Adressen und Cookies

In ihrer Stellungnahme (WP 136) zum Begriff „personenbezogene Daten“ hat die Arbeitsgruppe einige Klarstellungen in Bezug auf die Definition „personenbezogene Daten“ vorgenommen.¹⁰ Bei der Suchhistorie einer Person handelt es sich um personenbezogene Daten, wenn die Person, auf die sich die Daten beziehen, bestimmbar ist. Obwohl die IP-Adressen in den meisten Fällen von den Suchmaschinen nicht direkt bestimmbar sind, kann eine Identifizierung dennoch durch Dritte erfolgen. Internet-Diansteanbieter speichern IP-Adressdaten. Strafverfolgungs- und nationale Sicherheitsbehörden können Zugriff auf diese Daten erhalten, und in einigen Mitgliedstaaten haben auch bereits Privatparteien durch Zivilprozesse Zugriff darauf erhalten. In den meisten Fällen – einschließlich Fällen mit dynamischer IP-Adresszuordnung – sind also die notwendigen Daten zur Identifizierung des Benutzers bzw. der Benutzer der IP-Adresse vorhanden.

Die Arbeitsgruppe weist in ihrem Arbeitspapier Nr. 136 auf Folgendes hin: „*Wenn der Internet-Diansteanbieter also nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmaren Benutzern gehören, muss er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln.*“

Cookies

Wenn ein Cookie eine eindeutige Benutzererkennung enthält, handelt es sich bei dieser Kennung eindeutig um personenbezogene Daten. Dauerhafte Cookies oder ähnliche Mittel mit einer eindeutigen Benutzererkennung ermöglichen die Verfolgung der Benutzer eines bestimmten Computers selbst bei Verwendung dynamischer IP-Adressen.¹¹ Die Verhaltensdaten, die durch den Einsatz dieser Mittel generiert werden, ermöglichen eine noch stärkere Fokussierung auf die persönlichen Merkmale der betreffenden Person. Dies entspricht der grundlegenden Logik des vorherrschenden Geschäftsmodells.

¹⁰ WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf

¹¹ WP 136: „An diesem Punkt ist anzumerken, dass Personen in der Praxis zwar überwiegend anhand ihres Namens identifiziert werden, ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist. Beispielsweise kann eine Person anhand anderer „Kennzeichen“ singularisiert werden. So ordnen rechnergestützte Dateien zur Erfassung personenbezogener Daten den erfassten Personen gewöhnlich ein eindeutiges Kennzeichen zu, um Verwechslungen zwischen zwei Personen in der Datei auszuschließen.“

Für die Verarbeitung Verantwortlicher

Ein Suchmaschinenbetreiber, der Benutzerdaten einschließlich der IP-Adressen und/oder dauerhafter Cookies mit eindeutiger Kennung verarbeitet, fällt unter die Definition des für die Verarbeitung Verantwortlichen, da er über die Zwecke und Mittel der Verarbeitung entscheidet. Das multinational ausgerichtete Geschäftsmodell der großen Suchmaschinenbetreiber – oftmals mit Hauptsitzen außerhalb des EWR, weltweiten Dienstleistungsangeboten, Beteiligung verschiedener Zweigstellen und eventuell auch Dritter an der Verarbeitung personenbezogener Daten – hat die Frage aufgeworfen, wer bei einer Verarbeitung von personenbezogenen Daten als der für die Verarbeitung Verantwortliche anzusehen ist.

Die Arbeitsgruppe möchte an dieser Stelle den Unterschied zwischen den Definitionen des Datenschutzrechts im EWR und der Frage betonen, ob das Datenschutzrecht in einer bestimmten Situation anwendbar ist. Ein Suchmaschinenbetreiber, der personenbezogene Daten wie z. B. Protokolle mit personenbezogenen Suchhistorien verarbeitet, ist für diese personenbezogenen Daten der für die Verarbeitung Verantwortliche unabhängig von der Frage nach der hoheitsrechtlichen Zuständigkeit.

Artikel 4 der Datenschutzrichtlinie / Anwendbares einzelstaatliches Recht

Artikel 4 der Datenschutzrichtlinie befasst sich mit der Frage nach dem anwendbaren einzelstaatlichen Recht. In ihrem „**Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU**“¹² hat die Arbeitsgruppe weitere Leitlinien in Bezug auf die Bestimmungen von Artikel 4 formuliert. Hinter dieser Bestimmung stehen zwei Erwägungsgründe. Erstens geht es darum, Lücken im bestehenden System des gemeinschaftlichen Datenschutzes zu schließen und eine Umgehung dieses Systems zu vermeiden. Zweitens geht es darum, die Möglichkeit auszuschließen, dass ein und derselbe Verarbeitungsvorgang den Rechtsvorschriften von mehr als einem EU-Mitgliedstaat unterliegt. Aufgrund des multinationalen Charakters der von den Suchmaschinen ausgelösten Datenströme befasst sich die Arbeitsgruppe mit beiden Sachverhalten.

Bei der Verarbeitung personenbezogener Daten durch einen Suchmaschinenbetreiber, der in einem oder in mehreren Mitgliedstaaten niedergelassen ist und all seine Dienstleistungen dort erbringt, fällt die Verarbeitung personenbezogener Daten eindeutig in den Anwendungsbereich der Datenschutzrichtlinie. In diesem Fall ist es wichtig zu beachten, dass die Datenschutzbestimmungen nicht auf die betroffenen Personen im Hoheitsgebiet oder mit einer Staatsangehörigkeit eines der Mitgliedstaaten beschränkt sind.

Ist der Suchmaschinenbetreiber ein nicht im EWR ansässiger für die Verarbeitung Verantwortlicher, so ist das gemeinschaftliche Datenschutzrecht in zwei Fällen dennoch anwendbar, und zwar erstens, wenn der Suchmaschinenbetreiber eine Niederlassung in einem Mitgliedstaat im Sinne von Artikel 4 Absatz 1 Buchstabe a besitzt, und zweitens, wenn die Suchmaschine auf Mittel im Hoheitsgebiet eines Mitgliedstaats im Sinne von Artikel 4 Absatz 1 Buchstabe c zurückgreift. Im zweiten Fall muss der Suchmaschinenbetreiber gemäß Artikel 4 Absatz 2 einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter benennen.

¹² WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_de.pdf

Niederlassung im Hoheitsgebiet eines Mitgliedstaats (EWR)

Gemäß Artikel 4 Absatz 1 Buchstabe a ist das Datenschutzrecht eines Mitgliedstaats anzuwenden, wenn bei der Verarbeitung personenbezogener Daten bestimmte Vorgänge durch den für die Verarbeitung Verantwortlichen „im Rahmen der Tätigkeiten einer Niederlassung“ ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt. Als Ausgangspunkt sollte ein bestimmter Verarbeitungsvorgang für personenbezogene Daten gewählt werden. Bei der Anwendung des Datenschutzrechts auf eine bestimmte Suchmaschine, deren Hauptsitz sich außerhalb des EWR befindet, muss die Frage beantwortet werden, ob Niederlassungen im Hoheitsgebiet eines Mitgliedstaats an der Verarbeitung von Benutzerdaten beteiligt sind.

Wie die Arbeitsgruppe bereits in ihrem früheren Arbeitspapier¹³ dargelegt hat, setzt eine „Niederlassung“ die effektive und tatsächliche Ausübung einer Tätigkeit unter dauerhaften Bedingungen voraus und muss in Übereinstimmung mit der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften bestimmt werden. Die Rechtsform der Niederlassung – eine Geschäftsstelle, eine Tochtergesellschaft mit Rechtspersönlichkeit oder eine Vertretung durch Dritte – ist dabei nicht entscheidend.

Eine weitere Forderung ist jedoch, dass der Verarbeitungsvorgang „im Rahmen der Tätigkeiten“ einer Niederlassung ausgeführt wird. Das bedeutet, dass die Niederlassung ebenfalls eine bedeutende Rolle bei dem betreffenden Verarbeitungsvorgang spielen sollte. Dies ist eindeutig der Fall, wenn:

- eine Niederlassung für die Beziehungen zu den Benutzern der Suchmaschine in einem bestimmten gerichtlichen Zuständigkeitsbereich verantwortlich ist;
- ein Suchmaschinenbetreiber ein Büro in einem Mitgliedstaat (EWR) einrichtet, das am Verkauf zielgruppenspezifischer Werbeanzeigen an die Einwohner dieses Staates beteiligt ist;
- die Niederlassung eines Suchmaschinenbetreibers in Bezug auf Benutzerdaten richterlichen Anordnungen und/oder Ersuchen der zuständigen Behörden eines Mitgliedstaats zur Strafverfolgung nachkommt.

Die Verantwortung für die Klärung, inwieweit die Niederlassungen im Hoheitsgebiet der Mitgliedstaaten an der Verarbeitung personenbezogener Daten beteiligt sind, liegt beim Suchmaschinenbetreiber. Ist eine nationale Niederlassung an der Verarbeitung von Benutzerdaten beteiligt, so ist Artikel 4 Absatz 1 Buchstabe a der Datenschutzrichtlinie anwendbar.

Nicht im EWR ansässige Suchmaschinenbetreiber sollten ihre Benutzer darüber informieren, welche Bedingungen – das Vorhandensein einer Niederlassung oder die Verwendung von Mitteln – sie zur Einhaltung der Datenschutzrichtlinie verpflichten.

Verwendung von Mitteln

Suchmaschinen, die im Hoheitsgebiet eines Mitgliedstaats (EWR) für die Verarbeitung von personenbezogenen Daten auf Mittel zurückgreifen, fallen ebenfalls in den Anwendungsbereich der Datenschutzgesetze dieses Mitgliedstaats. Die

¹³ WP 56, S. 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_de.pdf

Datenschutzgesetze eines Mitgliedstaats sind auch noch anwendbar, wenn der für die Verarbeitung Verantwortliche „[...] zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchführung durch das Gebiet der Europäischen Gemeinschaft verwendet werden.“

Was die Bereitstellung von Suchmaschinendiensten außerhalb der EU anbetrifft, so können im Hoheitsgebiet eines Mitgliedstaats befindliche Datenzentren für die Speicherung und Fernverarbeitung personenbezogener Daten genutzt werden. Weitere Beispiele für Mittel sind der Einsatz von Personalcomputern, Endgeräten und Servern. Die Verwendung von Cookies und ähnlichen Softwareinstrumenten durch einen Anbieter von Online-Diensten kann ebenfalls als Rückgriff auf Mittel im Hoheitsgebiet eines Mitgliedstaats angesehen werden, was somit die Anwendung der Datenschutzgesetze des betreffenden Mitgliedstaats erfordert. Dieser Punkt wurde im weiter oben erwähnten Arbeitspapier (WP 56) erörtert: „Wie bereits gesagt, kann der PC eines Nutzers als ein Mittel im Sinne von Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG angesehen werden. Er befindet sich im Gebiet eines Mitgliedstaats. Der für die Verarbeitung Verantwortliche hat beschlossen, dieses Mittel zum Zwecke der Verarbeitung personenbezogener Daten zu nutzen. Wie bereits in den vorstehenden Absätzen erläutert, laufen jetzt einige technische Operationen ab, die nicht unter der Kontrolle der betroffenen Person stehen. Der für die Verarbeitung Verantwortliche verfügt damit über die Mittel des Nutzers und diese Mittel werden nicht nur zum Zwecke der Durchführung durch das Gebiet der Gemeinschaft verwendet.“

Schlussfolgerung

Aus der kombinierten Wirkung der Artikel 4 Absatz 1 Buchstabe a und Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie ergibt sich, dass deren Bestimmungen auf die Verarbeitung personenbezogener Daten durch Suchmaschinenbetreiber in vielen Fällen anwendbar sind, auch wenn sich ihr Hauptsitz außerhalb des EWR befindet.

Welches innerstaatliche Recht in einem bestimmten Fall anwendbar ist, ist Gegenstand einer weiteren Analyse der Fakten des betreffenden Falls. Die Arbeitsgruppe erwartet von den Suchmaschinenbetreibern eine Beteiligung an dieser Analyse, indem sie ihre Rolle und Tätigkeit im EWR in angemessener Weise klären.

Für multinationale Suchmaschinenbetreiber gilt:

- Ein Mitgliedstaat, in dem der Suchmaschinenbetreiber eine Niederlassung besitzt, wendet sein innerstaatliches Datenschutzrecht auf die Verarbeitung gemäß Artikel 4 Absatz 1 Buchstabe a an;
- wenn der Suchmaschinenbetreiber in keinem der Mitgliedstaaten ansässig ist, wendet ein Mitgliedstaat sein innerstaatliches Datenschutzrecht auf die Verarbeitung gemäß Artikel 4 Absatz 1 Buchstabe c an, wenn das Unternehmen im Hoheitsgebiet des Mitgliedstaats¹⁴ zum Zwecke der Verarbeitung

¹⁴ Bei der Beurteilung, ob Artikel 4 Absatz 1 Buchstabe c in Bezug auf die Verwendung von Cookies geltend gemacht werden kann, legt die Arbeitsgruppe die folgenden Kriterien zugrunde: Das erste Kriterium ist die Situation, in der ein Suchmaschinenbetreiber eine Niederlassung in einem Mitgliedstaat besitzt, Artikel 4 Absatz 1 Buchstabe a aber nicht anwendbar ist, weil diese Niederlassung keine wesentliche Rolle bei der Datenverarbeitung spielt (z. B. ein Pressevertreter). Weitere Kriterien sind die Entwicklung und/oder Gestaltung länderspezifischer

personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift (beispielsweise durch Verwendung von Cookies).

In bestimmten Fällen wird ein multinationaler Suchmaschinenbetreiber aufgrund der Regelungen für das anwendbare Recht und der länderübergreifenden Dimension bei der Verarbeitung personenbezogener Daten gleich mehrere Datenschutzgesetze einzuhalten haben:

- Ein Mitgliedstaat wendet sein innerstaatliches Recht auf eine außerhalb des EWR ansässige Suchmaschine an, wenn diese auf Mittel zurückgreift;
- ein Mitgliedstaat kann sein innerstaatliches Recht nicht auf eine im EWR ansässige und einer anderen hoheitsrechtlichen Zuständigkeit unterliegende Suchmaschine anwenden, auch wenn die Suchmaschine auf Mittel zurückgreift. In derartigen Fällen ist das innerstaatliche Recht des Mitgliedstaats anzuwenden, in dem der Suchmaschinenbetreiber niedergelassen ist.

4.1.3 Anwendbarkeit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten)

Suchmaschinendienste im engeren Sinne fallen allgemein nicht unter den neuen Regelungsrahmen für elektronische Kommunikation, zu dem die Datenschutzrichtlinie für elektronische Kommunikation gehört. Artikel 2 Buchstabe c der Rahmenrichtlinie (2002/21/EG), die einige allgemeine Begriffsbestimmungen für den Regelungsrahmen enthält, schließt Dienste ausdrücklich aus, die Inhalte anbieten oder eine redaktionelle Kontrolle über Inhalte ausüben:

„Elektronische Kommunikationsdienste“: gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und –dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;

Suchmaschinen fallen somit nicht unter die Definition für elektronische Kommunikationsdienste.

Ein Suchmaschinenbetreiber kann jedoch einen Zusatzdienst anbieten, der unter die Definition für einen elektronischen Kommunikationsdienst fällt, etwa einen öffentlich zugänglichen Dienst für elektronische Post, der der Richtlinie 2002/58/EG für elektronische Kommunikation und der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten unterliegen würde.

Suchmaschinendienste, die tatsächlichen Kenntnisse des Anbieters von Online-Diensten im Umgang mit den Benutzern, die in diesem Land ansässig sind, sowie der Vorteil eines dauerhaften Anteils am Benutzermarkt in einem bestimmten Mitgliedstaat.

In Artikel 5 Absatz 2 der Richtlinie über die Vorratsspeicherung von Daten heißt es ausdrücklich: „Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.“ Demzufolge wären Suchanfragen als Inhaltsdaten und nicht als Verkehrsdaten zu qualifizieren, und die Richtlinie würde ihre Speicherung auf Vorrat somit nicht rechtfertigen.

Jegliche Bezugnahmen auf die Richtlinie über die Vorratsspeicherung von Daten in Verbindung mit der Speicherung von Server-Protokollen, die von einem Suchmaschinendienst generiert werden, gehen folglich fehl.

Artikel 5 Absatz 3 und Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation

Einige Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation wie Artikel 5 Absatz 3 (Cookies und Spyware) und Artikel 13 (unerbetene Nachrichten) sind allgemeine Bestimmungen, die nicht nur auf die elektronische Kommunikationsdienste anwendbar sind, sondern auch auf andere Dienste, in denen diese Techniken verwendet werden.

Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, die im Zusammenhang mit Erwägungsgrund 25 dieser Richtlinie zu lesen ist, befasst sich mit der Speicherung von Informationen im Endgerät eines Teilnehmers oder Nutzers. Die Verwendung dauerhafter Cookies mit eindeutigen Kennungen bietet die Möglichkeit, die Nutzung eines bestimmten Computers zu verfolgen und ein entsprechendes Profil zu erstellen, selbst wenn dynamische IP-Adressen verwendet werden. Artikel 5 Absatz 3 und Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation legen eindeutig dar, dass die Speicherung derartiger Informationen im Endgerät der Nutzer, d. h. Cookies und ähnliche Instrumente (kurz: Cookie), im Einklang mit den Bestimmungen der Datenschutzrichtlinie stehen muss. Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation klärt somit die Verpflichtungen hinsichtlich der Verwendung von Cookies durch einen Dienst der Informationsgesellschaft aufgrund der Datenschutzrichtlinie.

4.2 Anbieter von Inhalten

Die Suchmaschinen verarbeiten Informationen, einschließlich personenbezogener Daten, indem sie das Internet und andere Quellen, die sie durchsuchbar und durch diese Dienste einfach zugänglich machen, durchforsten, analysieren und indexieren. Einige Suchmaschinendienste veröffentlichen Daten in einem so genannten „Cache“ (Zwischenspeicher) neu.

4.2.1. Freie Meinungsäußerung und Recht auf Privatsphäre

Die Arbeitsgruppe ist sich der besonderen Rolle von Suchmaschinen in der Online-Informationsumgebung bewusst. Beim gemeinschaftlichen Datenschutzrecht und bei den Rechtsvorschriften der verschiedenen Mitgliedstaaten geht es darum, ein Gleichgewicht zwischen dem Schutz des Rechts auf Privatsphäre und dem Schutz personenbezogener Daten einerseits und dem ungehinderten Informationsfluss und dem Grundrecht auf freie Meinungsäußerung andererseits zu finden.

Artikel 9 der Datenschutzrichtlinie soll garantieren, dass dieses Gleichgewicht in den Rechtsvorschriften der Mitgliedstaaten im Kontext der Medien gefunden wird. Außerdem hat der Europäische Gerichtshof klargestellt, dass die Grenzen der freien Meinungsäußerung, die sich aus der Anwendung der Datenschutzgrundsätze ableiten, mit dem geltenden Recht im Einklang stehen und den Grundsatz der Verhältnismäßigkeit beachten müssen.¹⁵

4.2.2 Datenschutzrichtlinie

Die Datenschutzrichtlinie enthält keine spezielle Bezugnahme auf die Verarbeitung personenbezogener Daten durch Dienste der Informationsgesellschaft, die als Vermittler handeln. Das entscheidende Kriterium in der Datenschutzrichtlinie (95/46/EG) für die Anwendbarkeit der Datenschutzbestimmungen ist die Definition des für die Verarbeitung Verantwortlichen, nämlich ob eine bestimmte Stelle „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Die Frage, ob ein Vermittler als der eigentliche für die Verarbeitung Verantwortliche anzusehen ist, oder aber als eine Stelle, die gemeinsam mit anderen für eine bestimmte Verarbeitung von personenbezogenen Daten verantwortlich ist, ist getrennt von der Frage der Haftung für eine derartige Verarbeitung zu betrachten.¹⁶

Nach dem Grundsatz der Verhältnismäßigkeit ist ein Suchmaschinenbetreiber, der ausschließlich als Vermittler handelt, nicht als der Hauptverantwortliche für die inhaltliche Verarbeitung von personenbezogenen Daten anzusehen. In diesem Fall liegt die Hauptverantwortung für die Verarbeitung von personenbezogenen Daten beim Informationsanbieter.¹⁷ Die formale, rechtliche und praktische Kontrolle des Suchmaschinenbetreibers über die personenbezogenen Daten beschränkt sich in der Regel auf die Möglichkeit, Daten von ihren Servern zu entfernen. Was die Entfernung von personenbezogenen Daten aus ihrem Index und ihren Suchergebnissen anbetrifft, so verfügen die Suchmaschinenbetreiber über eine ausreichende Kontrolle, um sie hier als für die Verarbeitung Verantwortliche (allein oder gemeinsam mit anderen) anzusehen. In welchem Umfang sie jedoch zur Entfernung oder Sperrung von personenbezogenen

¹⁵ Der Europäische Gerichtshof hat zur Verhältnismäßigkeit der Wirkung der Datenschutzbestimmungen, d. h. zur freien Meinungsäußerung, in seinem Urteil in der Rechtssache Lindqvist gegen Schweden, Randnr. 88-90, ausführlich Stellung bezogen.

¹⁶ In einigen Mitgliedstaaten gibt es spezielle Ausnahmeregelungen auf horizontaler Ebene („sichere Häfen“) in Bezug auf die Haftung von Suchmaschinen („Instrumente zur Lokalisierung von Informationen“). Die Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) sieht zwar keine sicheren Häfen für Suchmaschinen vor, doch wurden in einigen Mitgliedstaaten dennoch entsprechende Regelungen umgesetzt. Siehe dazu „Erster Bericht über die Anwendung der 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“), 21.11.2003, KOM(2003) 702 endg., S. 13.

¹⁷ Streng genommen könnten die Benutzer des Suchmaschinendienstes ebenfalls als für die Verarbeitung Verantwortliche angesehen werden, doch ihre Rolle liegt als „ausschließlich persönliche Tätigkeit“ in der Regel außerhalb des Anwendungsbereichs der Richtlinie (siehe Artikel 3 Absatz 2, zweiter Spiegelstrich).

Daten verpflichtet sind, hängt womöglich vom allgemeinen Deliktrecht und von den Haftungsvorschriften des jeweiligen Mitgliedstaats ab.¹⁸

Eigentümer von Websites können mit Hilfe der Datei *robots.txt* oder der Merker *Noindex/NoArchive* von vornherein ihre Nichtbeteiligung („Opt-out“) an Suchmaschinen und an der Zwischenspeicherung erklären.¹⁹ Es ist sehr wichtig, dass die Suchmaschinenbetreiber derartigen Nichtbeteiligungsklauseln von Website-Herausgebern Beachtung schenken. Diese Nichtbeteiligung kann vor der ersten Durchsuchung („Crawling“) der Website oder auch nach ihrer Durchsuchung angegeben werden; im zuletzt genannten Fall sollte die Suchmaschine so schnell wie möglich einen Aktualisierungslauf durchführen.

Suchmaschinenbetreiber beschränken sich nicht immer auf eine reine Vermittlertätigkeit. Beispielsweise speichern einige Suchmaschinen komplette Web-Inhalte – einschließlich der darin enthaltenen personenbezogenen Daten – auf ihren Servern. Außerdem ist unklar, inwieweit die Suchmaschinen in den von ihnen verarbeiteten Inhalten aktiv nach personenbezogenen Daten suchen. Die Durchsuchung, Analyse und Indexierung kann automatisch erfolgen, ohne das Vorhandensein von personenbezogenen Daten zu offenbaren. Spezielle Arten von personenbezogenen Daten wie beispielsweise Sozialversicherungsnummern, Kreditkartennummern, Telefonnummern und Adressen für elektronische Post können aufgrund ihres Formats jedoch einfach ermittelt werden. Es gibt aber auch höher entwickelte Technologien, die von den Suchmaschinenbetreibern in zunehmendem Maße eingesetzt werden. Dazu gehören beispielsweise die Technologie zur Gesichtserkennung im Zusammenhang mit der Bildverarbeitung und Bildsuche.

Auf diese Weise können die Suchmaschinenbetreiber Mehrwert schaffende Vorgänge durchführen, die mit den Merkmalen oder Arten von personenbezogenen Daten in den verarbeiteten Informationen verknüpft sind. In diesen Fällen trägt der Suchmaschinenbetreiber im Rahmen der Datenschutzgesetze die volle Verantwortung für den Inhalt, der aus der Verarbeitung personenbezogener Daten resultiert. Die gleiche Verantwortlichkeit gilt für einen Suchmaschinenbetreiber, der Werbeanzeigen verkauft, die aufgrund personenbezogener Daten – beispielsweise des Namens einer Person – geschaltet werden.

Die Caching-Funktionalität

Die Caching-Funktionalität ist eine weitere Möglichkeit für Suchmaschinenbetreiber, über ihre Rolle als reine Informationsvermittler hinauszugehen. Die Speicherungsfrist von Inhalten in einem Cache-Speicher sollte auf den Zeitraum begrenzt werden, der zur

¹⁸ In einigen EU-Mitgliedstaaten haben die Datenschutzbehörden spezielle Regelungen für die Verantwortlichkeit von Suchmaschinenbetreibern erlassen, Inhaltsdaten vom Suchindex zu entfernen. Diese Regelungen beruhen auf dem in Artikel 14 der Datenschutzrichtlinie (95/46/EG) verankerten Widerspruchsrecht und auf der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG). Gemäß diesen einzelstaatlichen Rechtsvorschriften sind die Suchmaschinenbetreiber verpflichtet, ein Verfahren zur Meldung und Entfernung rechtswidriger Inhalte ähnlich wie Hosting-Anbieter einzuhalten, damit sie von der Haftung freigestellt bleiben.

¹⁹ Dies kann mehr als eine optionale Lösung sein. Veröffentlichender von personenbezogenen Daten müssen sich mit der Frage befassen, ob ihre Rechtsgrundlage für die Veröffentlichung die Indexierung dieser Informationen durch Suchmaschinen einschließt, und gegebenenfalls entsprechende Schutzmechanismen vorsehen, unter anderem durch Verwendung der Datei *robots.txt* und/oder *Noindex/NoArchive*-Merker.

Lösung des Problems der vorübergehenden Nichtverfügbarkeit der eigentlichen Website notwendig ist.

Jegliche Zwischenspeicherung von auf indexierten Websites enthaltenen, personenbezogenen Daten über diesen aus Gründen der technischen Verfügbarkeit notwendigen Zeitraum hinaus ist als eine unabhängige Neuveröffentlichung anzusehen. Nach Auffassung der Arbeitsgruppe liegt die Verantwortung für die Einhaltung der Datenschutzgesetze hier beim Anbieter derartiger Caching-Funktionalitäten in seiner Rolle als Verantwortlicher für die Verarbeitung der personenbezogenen Daten, die in den zwischengespeicherten Veröffentlichungen enthalten sind. Falls die ursprüngliche Veröffentlichung geändert wird, etwa um unrichtige personenbezogene Daten zu entfernen, sollte der Verantwortliche für die Verarbeitung der Cache-Inhalte umgehend auf Aufforderungen zur Aktualisierung des Cache-Kopie reagieren oder die Cache-Kopie vorübergehend sperren, bis die Website von der Suchmaschine erneut durchsucht wird.

5. RECHTMÄSSIGKEIT DER VERARBEITUNG

Artikel 6 der Datenschutzrichtlinie sieht vor, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden, für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Außerdem müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen. Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, muss gemäß Artikel 7 dieser Richtlinie mindestens eine der sechs Voraussetzungen für die Zulässigkeit der Verarbeitung erfüllt sein.

5.1. Von den Suchmaschinenbetreibern vorgebrachte Zwecke und Gründe

Für die Verwendung und Speicherung von personenbezogenen Daten führen die Suchmaschinenbetreiber in ihrer Rolle als für die Verarbeitung Verantwortliche allgemein die folgenden Zwecke und Gründe an.

Verbesserung des Dienstes

Viele Suchmaschinenbetreiber verwenden Server-Protokolle, um ihr Dienstleistungsangebot und die Qualität ihrer Suchdienste zu verbessern. Sie sehen die Auswertung der Server-Protokolle als ein wichtiges Instrument, um die Qualität der Suchvorgänge, Ergebnisse und Werbung zu verbessern und neue, noch nicht näher bestimmbare Dienste zu entwickeln.

Systemsicherheit

Server-Protokolle tragen nach Auskunft der Betreiber zur Sicherheit der Suchmaschinendienste bei. Einige Suchmaschinenbetreiber erklärten, dass die Speicherung von Protokollen zum Schutz des Systems vor Sicherheitsangriffen beitragen kann und eine aussagekräftige Stichprobe an Server-Protokolldaten notwendig ist, um wiederkehrende Muster zu erkennen und Sicherheitsbedrohungen zu analysieren.

Betrugsbekämpfung

Server-Protokolle schützen die Systeme und Benutzer der Suchmaschinen angeblich vor Betrug und Missbrauch. Viele Suchmaschinenbetreiber betreiben einen „Pay-per-Click“-Mechanismus für die angezeigte Werbung. Ein Nachteil dieses Systems ist jedoch, dass einem Unternehmen zu Unrecht Gebühren in Rechnung gestellt werden können, wenn ein Angreifer mit Hilfe automatischer Software systematisch auf die Werbeanzeigen klickt. Die Suchmaschinenbetreiber achten zunehmend darauf, dass ein derartiges Verhalten aufgedeckt und beseitigt wird.

Abrechnungsanforderungen werden als Zweck für Dienste wie Klicks auf gesponserte Links angeführt, wenn aus Abrechnungsgründen eine vertragliche Verpflichtung zur Datenspeicherung besteht, und zwar mindestens bis zur Begleichung der Rechnungen und bis zum Ablauf der Frist für Rechtsstreitigkeiten.

Personalisierte Werbung

Zur Erhöhung ihrer Einnahmen streben die Suchmaschinenbetreiber eine personalisierte Werbung an. Gegenwärtig werden unter anderem die bisherigen Suchanfragen, Benutzerkategorien sowie geografische Kriterien berücksichtigt. Daher kann auf Basis des bisherigen Benutzerverhaltens und der IP-Adresse des Benutzers personalisierte Werbung angezeigt werden.

Einige Suchmaschinen erstellen auch Statistiken um zu bestimmen, welche Benutzerkategorien auf welche Informationen zu welcher Zeit online zugreifen. Diese Daten können für die Verbesserung der Dienste, für zielgruppenspezifische Werbung sowie für kommerzielle Zwecke verwendet werden, um die Kosten für ein Unternehmen zu ermitteln, das für seine Produkte im Internet werben möchte.

Strafverfolgung

Nach Angaben einiger Betreiber stellen Protokolle ein wichtiges Instrument für die Strafverfolgung dar, um schwere Straftaten wie Kindesmissbrauch untersuchen und strafrechtlich verfolgen zu können.

5.2. Analyse der Zwecke und Gründe durch die Arbeitsgruppe

Generell ist festzustellen, dass die Suchmaschinenbetreiber keinen umfassenden Überblick geben, für welche festgelegten, eindeutigen und rechtmäßigen Zwecke sie personenbezogene Daten verarbeiten. Erstens sind einige Zwecke wie „Verbesserung der Dienste“ oder „personalisierte Werbung“ zu allgemein definiert und bieten daher keinen angemessenen Beurteilungsrahmen für die Rechtmäßigkeit der Zwecke. Da zahlreiche Suchmaschinenbetreiber viele verschiedene Verarbeitungszwecke anführen, ist zweitens nicht klar, in welchem Umfang Daten für einen anderen Zweck weiterverarbeitet werden, der mit der ursprünglichen Zweckbestimmung nicht vereinbar ist.

Die Erhebung und Verarbeitung von personenbezogenen Daten kann unter einer oder mehreren Voraussetzungen rechtmäßig sein. Es gibt drei Gründe, auf die sich die Suchmaschinenbetreiber für verschiedene Zwecke berufen können.

- Einwilligung – Artikel 7 Buchstabe a der Datenschutzrichtlinie

Die Dienste der meisten Suchmaschinenbetreiber können sowohl ohne als auch mit Registrierung genutzt werden. Im zweiten Fall (wenn ein Benutzer beispielsweise ein spezifisches Benutzerkonto angelegt hat) kann die Einwilligung²⁰ als zulässiger Grund für die Verarbeitung bestimmter, festgelegter Kategorien von personenbezogenen Daten für festgelegte, rechtmäßige Zwecke, einschließlich der Speicherung der Daten für einen begrenzten Zeitraum, angeführt werden. Bei anonymen Benutzern des Dienstes und den personenbezogenen Daten von Benutzern, die sich gegen eine freiwillige Authentifizierung entschieden haben, kann freilich nicht von einer Einwilligung ausgegangen werden. Derartige Daten dürfen nicht für Zwecke verarbeitet oder gespeichert werden, die über die Anzeige einer Liste von Suchergebnissen für eine spezifische Suchanfrage hinausgehen.

- Erforderlich für die Erfüllung eines Vertrags – Artikel 7 Buchstabe b der Datenschutzrichtlinie

Eine Verarbeitung kann auch erforderlich sein für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen. Auf diese Rechtsgrundlage können sich Suchmaschinenbetreiber bei der Erhebung von personenbezogenen Daten berufen, die ein Benutzer freiwillig angibt, um sich bei einem bestimmten Dienst, beispielsweise bei einem Benutzerkonto, anzumelden. Ähnlich wie im Falle der Einwilligung kann diese Rechtsgrundlage für die Verarbeitung bestimmter, festgelegter Kategorien von personenbezogenen Daten für festgelegte, rechtmäßige Zwecke von authentifizierten Benutzern angeführt werden.

Viele Internet-Unternehmen machen auch geltend, dass ein Benutzer bei der Nutzung der auf ihrer Website angebotenen Dienste, wie beispielsweise einer Suchmaske, faktisch eine vertragliche Beziehung eingeht. Eine derartige generelle Annahme erfüllt jedoch nicht die strenge Begrenzung auf die Erforderlichkeit, die in der Richtlinie gefordert wird.²¹

- Erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird – Artikel 7 Buchstabe f der Datenschutzrichtlinie

Gemäß Artikel 7 Buchstabe f der Richtlinie könnte die Verarbeitung zur Verwirklichung des berechtigten Interesses erforderlich sein, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

²⁰ Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie ist die Einwilligung der betroffenen Person „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.“

²¹ Artikel 7 Buchstabe b der Richtlinie: „... erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.“

Verbesserung der Dienste

Einige Suchmaschinenbetreiber speichern den Inhalt von Benutzeranfragen in ihren Server-Protokollen. Diese Informationen stellen ein wichtiges Instrument für Suchmaschinenbetreiber dar. Sie ermöglichen ihnen die Verbesserung ihrer Dienste durch die Analyse der Art von Suchanfragen und deren Verfeinerung und durch die Auswertung der von den Benutzern weiterverfolgten Suchergebnisse. Die Artikel-29-Arbeitsgruppe hält die Zuordnung der Suchanfragen zu identifizierbaren Personen jedoch nicht für zwingend erforderlich, damit die Betreiber ihre Suchdienste verbessern können.

Um die Aktionen eines einzelnen Benutzers zu korrelieren (und auf diese Weise z. B. zu ermitteln, ob die Vorschläge der Suchmaschine hilfreich sind), ist lediglich eine Abgrenzung der Aktionen eines Benutzers bei einer bestimmten Suchanfrage von denen eines anderen Benutzers notwendig; die Identifizierung dieser Benutzer ist hingegen nicht notwendig. Beispielsweise könnte für eine Suchmaschine die Information aufschlussreich sein, dass Benutzer X nach „Woodhouse“ gesucht und anschließend auf die Ergebnisse für die angebotene orthografische Variante „Wodehouse“ geklickt hat – sie braucht aber nicht zu wissen, wer Benutzer X ist. Die Verbesserung der Dienste kann daher nicht als zulässiger Grund für die Speicherung nicht anonymisierter Daten angesehen werden.

Systemsicherheit

Die Suchmaschinenbetreiber könnten die Notwendigkeit zur Aufrechterhaltung der Sicherheit ihres Systems als berechtigtes Interesse und angemessenen Grund für die Verarbeitung personenbezogener Daten anführen. Personenbezogene Daten, die für Sicherheitszwecke gespeichert werden, müssen jedoch einer strengen Zweckbeschränkung unterliegen. Daher dürfen Daten, die für Sicherheitszwecke gespeichert werden, nicht für andere Zwecke, beispielsweise zur Optimierung eines Dienstes, verwendet werden. Die Suchmaschinenbetreiber argumentieren, dass die Speicherung der Server-Protokolle über einen angemessenen Zeitraum (die Anzahl der Monate ist von Suchmaschine zu Suchmaschine unterschiedlich) notwendig ist, damit sie typische Verhaltensmuster der Benutzer erkennen und folglich Überflutungsangriffe („Denial of Service“) und andere Sicherheitsbedrohungen ermitteln und abwehren können. Alle Suchmaschinenbetreiber sollten jedoch in der Lage sein, die gewählte Speicherungsfrist für diesen Zweck und die damit einhergehende Notwendigkeit zur Verarbeitung dieser Daten umfassend zu begründen.

Betrugsbekämpfung

Trotz des berechtigten Interesses der Suchmaschinenbetreiber an der Erkennung und Vermeidung von Betrugsdelikten wie etwa „Klick-Betrug“ sollte ebenso wie bei der Speicherung für Sicherheitszwecke die Menge der gespeicherten und verarbeiteten personenbezogenen Daten und die für diesen Zweck angesetzte Speicherungsfrist für personenbezogene Daten davon abhängen, ob die Daten für die Erkennung und Vermeidung von Betrugsdelikten tatsächlich notwendig sind.

Abrechnung

Die systematische Protokollierung üblicher Suchmaschinendaten, in denen der Benutzer nicht auf einen gesponserten Link geklickt hat, kann nicht mit Abrechnungsanforderungen gerechtfertigt werden. Ausgehend von den Antworten der Suchmaschinenbetreiber auf den Fragebogen hat die Arbeitsgruppe auch erhebliche Zweifel, dass personenbezogene Daten von Suchmaschinenbenutzern für

Abrechnungszwecke wirklich notwendig sind. Für eine schlüssige Beurteilung wären weitere Untersuchungen notwendig. Auf jeden Fall fordert die Arbeitsgruppe die Suchmaschinenbetreiber zur Entwicklung von Abrechnungsmechanismen auf, die mehr Rücksicht auf die Privatsphäre nehmen, beispielsweise durch Verwendung anonymisierter Daten.

Personalisierte Werbung

Suchmaschinenbetreiber, die personalisierte Werbung zur Steigerung ihrer Einnahmen anbieten möchten, können die Rechtmäßigkeit der Verarbeitung einiger personenbezogener Daten zwar mit Artikel 7 Buchstabe a der Richtlinie (Einwilligung) oder Artikel 7 Buchstabe b der Richtlinie (Erfüllung eines Vertrags) begründen, doch es ist schwierig, einen rechtmäßigen Grund für diese Praxis bei Benutzern zu finden, die nicht ihre ausdrückliche Einwilligung auf der Grundlage spezifischer Informationen über den Verarbeitungszweck gegeben haben. Die Arbeitsgruppe spricht sich eindeutig für anonymisierte Daten aus.

Strafverfolgung und Rechtsersuchen

Gelegentlich fordern Strafverfolgungsbehörden Benutzerdaten von Suchmaschinen an, um Straftaten aufzudecken oder zu verhindern. Auch Privatparteien könnten versuchen, einen Suchmaschinenbetreiber über eine richterliche Anordnung zur Herausgabe von Benutzerdaten zu veranlassen. Sofern derartige Rechtsersuchen die geltenden Rechtsverfahren einhalten und zu rechtsgültigen gerichtlichen Anordnungen führen, müssen Suchmaschinenbetreiber diese selbstverständlich befolgen und die benötigten Informationen liefern. Diese Einhaltung von Anordnungen sollte jedoch nicht mit einer rechtlichen Verpflichtung oder Rechtfertigung für die Speicherung derartiger Daten ausschließlich für diese Zwecke verwechselt werden.

Außerdem könnten große Bestände an personenbezogenen Daten in den Händen der Suchmaschinenbetreiber die Strafverfolgungsbehörden und andere Kreise dazu verleiten, ihre Rechte häufiger und mit mehr Nachdruck auszuüben, was wiederum zu einem Vertrauensverlust bei den Verbrauchern führen könnte.

5.3. Von der Branche zu klärende Fragen

Speicherungsfristen

Wenn die vom Suchmaschinenbetreiber durchgeführte Verarbeitung dem einzelstaatlichen Recht unterliegt, müssen dabei die Rechtsvorschriften des betreffenden Mitgliedstaats für den Schutz der Privatsphäre und die Speicherungsfristen eingehalten werden.

Bei der Speicherung personenbezogener Daten sollte die Speicherungsfrist nicht über den für die spezifischen Verarbeitungszwecke notwendigen Zeitraum hinausgehen. Folglich könnten am Ende einer Suchsitzung die personenbezogenen Daten gelöscht werden; eine fortgesetzte Speicherung müsste dann angemessen begründet werden. Einige Suchmaschinenbetreiber scheinen Daten jedoch auf unbestimmte Zeit zu speichern, was verboten ist. Für jeden Zweck sollte eine befristete Speicherdauer festgelegt werden. Außerdem sollte die zu speichernde Menge an personenbezogenen Daten nicht über den jeweiligen Zweck hinausgehen.

In der Praxis speichern die großen Suchmaschinenbetreiber die personenbezogenen Daten über ihre Benutzer in aller Regel über ein Jahr lang (die genauen Zeiten können abweichen). Die Arbeitsgruppe begrüßt die jüngsten Reduzierungen der Speicherungsfristen für personenbezogene Daten durch große Suchmaschinenbetreiber. Die Tatsache, dass führende Unternehmen in dieser Branche ihre Speicherungsfristen reduzieren konnten, deutet freilich darauf hin, dass die bisherigen Fristen länger als notwendig waren.

Angesichts der bisher abgegebenen Stellungnahmen der Suchmaschinenbetreiber zu den möglichen Zwecken für die Erhebung personenbezogener Daten sieht die Arbeitsgruppe keine Grundlage für eine Speicherungsfrist von mehr als sechs Monaten.²²

Die Speicherung von personenbezogenen Daten und die entsprechende Speicherungsfrist müssen immer (mit konkreten und relevanten Argumenten) begründbar sein und auf ein Minimum reduziert werden, um die Transparenz zu verbessern, eine Verarbeitung nach Treu und Glauben sicherzustellen und die Verhältnismäßigkeit für den Zweck zu gewährleisten, der eine derartige Speicherung rechtfertigt.

Daher fordert die Arbeitsgruppe die Suchmaschinenbetreiber dazu auf, den Grundsatz „Privacy by Design“ (entwurfsimmanenter Schutz der Privatsphäre) zu verwirklichen, der zur weiteren Reduzierung der Speicherungsfrist beitragen wird. Nach Auffassung der Arbeitsgruppe wird eine reduzierte Speicherungsfrist das Vertrauen der Benutzer in den Dienst stärken und folglich einen wichtigen Wettbewerbsvorteil darstellen.

Falls die Suchmaschinenbetreiber personenbezogene Daten länger als sechs Monate speichern, müssen sie umfassend nachweisen, dass dies für den Dienst zwingend notwendig ist.

In jedem Fall müssen die Suchmaschinenbetreiber die Benutzer über ihre jeweilige Speicherungspolitik für alle Arten der von ihnen verarbeiteten Benutzerdaten informieren.

Weiterverarbeitung für verschiedene Zwecke

In welchem Umfang und wie Benutzerdaten weiter analysiert und ob (detaillierte) Benutzerprofile erstellt werden, hängt vom Suchmaschinenbetreiber ab. Die Arbeitsgruppe ist sich der Möglichkeit bewusst, dass diese Art der Weiterverarbeitung von Benutzerdaten womöglich einen Kernbereich der Innovation der Suchmaschinentechologie berührt und für den Wettbewerb von großer Bedeutung sein kann. Die uneingeschränkte Offenlegung der Weiterverwendung und Analyse von Benutzerdaten könnte auch die Anfälligkeit der Suchmaschinendienste für den Missbrauch ihrer Dienste erhöhen. Derlei Erwägungen können jedoch nicht als Rechtfertigung für die Nichteinhaltung der anwendbaren Datenschutzgesetze der Mitgliedstaaten geltend gemacht werden. Außerdem können sich die Suchmaschinenbetreiber nicht darauf berufen, dass sie mit der Erhebung von personenbezogenen Daten die Entwicklung neuer Dienste bezwecken, deren genaue Art noch nicht feststeht. Aus Gründen der Fairness sollten die betroffenen Personen über den Umfang der möglichen Eingriffe in ihre Privatsphäre Bescheid wissen, wenn jemand

²² In den einzelstaatlichen Rechtsvorschriften kann die Löschung von personenbezogenen Daten auch zu einem früheren Zeitpunkt vorgeschrieben sein.

Kenntnis von ihren Daten erlangt. Dies wird aber nicht möglich sein, wenn die Zwecke nicht genauer definiert werden.

Cookies

Dauerhafte Cookies mit einer eindeutigen Benutzerkennung sind personenbezogene Daten und unterliegen daher den anwendbaren Datenschutzgesetzen. Die Verantwortung für deren Verarbeitung kann nicht auf die Verantwortung des Benutzers reduziert werden, bestimmte Vorsichtsmaßnahmen in seinen Browser-Einstellungen zu treffen. Der Suchmaschinenbetreiber entscheidet darüber, ob ein Cookie gespeichert wird, welcher Cookie gespeichert wird und für welche Zwecke er verwendet wird. Auch das von einigen Suchmaschinenbetreibern eingestellte Verfallsdatum von Cookies erscheint übermäßig lang. Beispielsweise setzen verschiedene Unternehmen Cookies, die erst nach vielen Jahren verfallen. Bei Verwendung eines Cookies sollte für das Cookie eine angemessene Lebensdauer gewählt werden, die zum einen ein verbessertes Surf-Erlebnis und zum anderen eine Befristung der Lebensdauer ermöglicht. Vor allem im Hinblick auf die Standardeinstellungen von Browsern ist es sehr wichtig, dass die Benutzer umfassend über die Verwendung und die Wirkung von Cookies informiert werden. Diese Information sollte stärker in den Vordergrund gerückt werden und nicht nur ein Bestandteil der Datenschutzerklärungen sein, die in der Suchmaschine nicht unbedingt auf Anhieb auffindbar sind.

Anonymisierung

Wenn es keinen rechtmäßigen Grund für die Verarbeitung bzw. für die Verwendung über die festgelegten rechtmäßigen Zwecke hinaus gibt, müssen die Suchmaschinenbetreiber die personenbezogenen Daten löschen. Statt die Daten zu löschen, können sie sie auch anonymisieren. Diese Anonymisierung muss jedoch vollständig unumkehrbar sein, damit die Datenschutzrichtlinie nicht länger greift.

Selbst dort, wo eine IP-Adresse und ein Cookie durch eine eindeutige Kennung ersetzt werden, ist die Identifizierung von Personen durch Korrelation von gespeicherten Suchanfragen möglich. Aus diesem Grund sollten dort, wo eine Anonymisierung statt Löschung der Daten erfolgt, die verwendeten Methoden sorgfältig geprüft und gründlich durchgeführt werden. Dies kann die Beseitigung von Teilen der Suchhistorie erfordern, um die Möglichkeit einer indirekten Identifizierung des Benutzers auszuschließen, der diese Suchvorgänge durchgeführt hat.

Bei der Anonymisierung von Daten sollte jegliche Möglichkeit der Identifizierung von Personen ausgeschlossen werden. Auszuschließen ist selbst das Kombinieren der anonymisierten Informationen eines Suchmaschinenbetreibers mit Informationen, die ein anderer Beteiligter gespeichert hat (beispielsweise ein Internet-Diensteanbieter). Derzeit schneiden einige Suchmaschinenbetreiber IPv4-Adressen ab, indem sie die letzte Achtergruppe entfernen, womit sie effektiv Informationen über den Internet-Diensteanbieter oder das Teilnetz des Benutzers speichern, ohne die Person direkt zu identifizieren. Die Aktivität könnte dann von einer beliebigen der 254 IP-Adressen ausgehen. Dies ist für eine Anonymisierungsgarantie möglicherweise aber nicht immer ausreichend.

Zudem muss die Anonymisierung oder Löschung der Protokolle rückwirkend erfolgen und alle relevanten Protokolle der Suchmaschine weltweit einschließen.

Dienstübergreifende Datenkorrelation

Viele Suchmaschinenbetreiber bieten den Benutzern die Möglichkeit, die Nutzung der Dienste über ein persönliches Konto zu personalisieren. Abgesehen von Suchfunktionen bieten sie Dienste wie elektronische Post und/oder andere Kommunikationswerkzeuge, wie beispielsweise Boten (Messenger) oder Chats, und soziale Vernetzungsinstrumente wie Internet-Tagebücher (Web-Blogs) oder soziale Communities. Das entsprechende Angebot kann zwar von Anbieter zu Anbieter unterschiedlich sein, doch ein gemeinsames Merkmal derartiger Dienste ist das ihnen zugrunde liegende Geschäftsmodell und die kontinuierliche Entwicklung neuer personalisierter Dienste.

Die Korrelation des Kundenverhaltens über verschiedene personalisierte Dienste eines Suchmaschinenbetreibers und mitunter auch über verschiedene Plattformen²³ hinweg wird aus technischer Sicht durch die Benutzung eines zentralen persönlichen Kontos erleichtert, kann aber auch durch andere Mittel auf Basis von Cookies oder anderen charakteristischen Merkmalen wie einzelnen IP-Adressen bewerkstelligt werden. Wenn eine Suchmaschine beispielsweise einen Zusatzdienst wie „Desktop-Suche“ anbietet, erhält die Suchmaschine Informationen über die (Inhalte der) Dokumente, die ein Benutzer erstellt oder anzeigt. Mit Hilfe dieser Daten können die Suchanfragen angepasst werden und genauere Ergebnisse liefern.

Nach Auffassung der Arbeitsgruppe ist das dienst- und plattformübergreifende Korrelieren von personenbezogenen Daten für authentifizierte Benutzer nur mit Einwilligung und nach angemessener Unterrichtung der Benutzer rechtmäßig.

Wenn ein Benutzer die Vorteile eines stärker personalisierten Suchdienstes nutzen möchte, sollte die Registrierung bei einem Suchmaschinenbetreiber freiwillig sein. Die Suchmaschinenbetreiber dürfen den Benutzer nicht zu der Annahme verleiten, dass die Nutzung ihres Dienstes ein personalisiertes Konto erfordert, indem sie nicht identifizierte Benutzer automatisch zu einem Anmeldeformular für ein personalisiertes Konto umleiten, da keine Notwendigkeit und somit auch kein zulässiger Grund für die Erhebung derartiger personenbezogenen Daten besteht, außer mit freier Willenserklärung des Benutzers.

Eine Korrelation kann auch bei nicht authentifizierten Benutzern auf Basis von IP-Adressen oder eindeutigen Cookies erfolgen, die von allen verschiedenen Diensten eines Suchmaschinenbetreibers erkannt werden können. Gewöhnlich geschieht dies automatisch, ohne dass sich der Benutzer einer derartigen Korrelation bewusst ist. Die heimliche Überwachung des Benutzerverhaltens und sicherlich auch privaten Verhaltens wie der Besuch von Websites steht nicht im Einklang mit den Grundsätzen einer rechtmäßigen Verarbeitung nach Treu und Glauben im Sinne der Datenschutzrichtlinie. Die Suchmaschinenbetreiber sollten sich klar zum Umfang der dienstübergreifenden Korrelation von Daten äußern und Korrelationen nur mit Einwilligung des Benutzers vornehmen.

Einige Suchmaschinenbetreiber räumen in ihren Datenschutzerklärungen ausdrücklich ein, dass sie die vom Benutzer bereitgestellten Daten mit Daten von Dritten anreichern, z. B. von anderen Unternehmen, die beispielsweise geografische Informationen an Bereiche von IP-Adressen oder Websites mit Werbeanzeigen anhängen, die vom

²³ Beispielsweise bei Microsoft von der webbasierten Suchmaschine bis hin zu der mit dem Internet verbundenen Hardware, die für Spielzwecke verkauft wird (Xbox).

Suchmaschinenbetreiber verkauft werden.²⁴ Diese Art der Korrelation kann rechtswidrig sein, wenn die betroffenen Personen bei der Erhebung ihrer personenbezogenen Daten nicht informiert werden und wenn ihnen keine einfachen Zugriffsmöglichkeiten auf ihre Personenprofile und das Recht auf Berichtigung oder Löschung bestimmter unrichtiger oder überflüssiger Datenelemente eingeräumt wird. Ist die betreffende Verarbeitung für die Bereitstellung des (Such-) Dienstes nicht notwendig, wäre für eine rechtmäßige Verarbeitung die Einwilligung des Benutzers erforderlich, die ohne Zwang und in Kenntnis der Sachlage gegeben wurde.

6. VERPFLICHTUNG ZUR INFORMATION DER BETROFFENEN PERSON

Die meisten Internet-Benutzer wissen nicht, dass große Datenmengen über ihr Suchverhalten verarbeitet werden und für welche Zwecke diese Daten genutzt werden. Wenn sie sich dieser Verarbeitung nicht bewusst sind, können sie auch keine Entscheidungen in Kenntnis der Sachlage treffen.

Die Verpflichtung zur Information der betroffenen Personen über die Verarbeitung ihrer Daten gehört zu den fundamentalen Grundsätzen der Datenschutzrichtlinie. Artikel 10 regelt die Bereitstellung dieser Informationen, wenn die Daten direkt bei der betroffenen Person erhoben wurden. Die für die Verarbeitung Verantwortlichen sind verpflichtet, der betroffenen Person die folgenden Informationen mitzuteilen:

- Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;
- Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind;
- weitere Informationen, beispielsweise betreffend
 - die Empfänger oder Kategorien der Empfänger der Daten;

²⁴ Beispielsweise weist Microsoft in seiner Online-Datenschutzerklärung auf Folgendes hin: „Bei der Registrierung für bestimmte Microsoft-Dienste werden Sie nach persönlichen Informationen gefragt. Die von uns erfassten Daten werden möglicherweise mit Informationen kombiniert, die von anderen Microsoft-Diensten oder anderen Unternehmen erfasst wurden.“ URL: <http://privacy.microsoft.com/de-de/default.aspx>. In der vollständigen Online-Datenschutzerklärung macht Microsoft hinsichtlich der gemeinsamen Verwendung von Daten mit Werbepartnern auf Folgendes aufmerksam: „We also deliver advertisements and provide website analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well.“ (Wie schalten auch Werbeanzeigen und stellen Website-Analysewerkzeuge auf anderen Sites und für andere Dienste als von Microsoft bereit. Außerdem können wir Informationen darüber erheben, wie oft die Sites Dritter angezeigt wurden.) URL: <http://privacy.microsoft.com/en-us/fullnotice.aspx>. Google weist in seiner Datenschutzerklärung auf Folgendes hin: „Wir können die über Sie erhobenen personenbezogenen Daten mit Daten von anderen Google-Diensten oder anderen Unternehmen kombinieren, um das Angebot für unsere Nutzer zu verbessern, z. B. durch individuell auf Sie zugeschnittene Inhalte.“ URL: <http://www.google.de/privacy.html>. Yahoo! weist in seiner Datenschutzerklärung auf Folgendes hin: „Yahoo! may combine information about you that we have with information we obtain from business partners or other companies.“ (Yahoo! kann die Informationen über Sie mit Informationen kombinieren, die wir von Geschäftspartnern oder anderen Unternehmen erhalten.) URL: <http://info.yahoo.com/privacy/us/yahoo/details.html>

- die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung;
- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten.

In ihrer Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten sollten die Suchmaschinenbetreiber gegenüber den Benutzern klarstellen, welche Informationen über sie erfasst werden und für welche Zwecke diese bestimmt sind. Bei der Erhebung von personenbezogenen Daten sollte deren Verwendung allgemein beschrieben werden, auch wenn an anderer Stelle eine detailliertere Beschreibung aufgeführt ist. Ebenso sollten die Benutzer über Software informiert werden, z. B. über Cookies, die auf ihrem Computer beim Zugriff auf eine Website gesetzt werden, und wie diese abgelehnt oder gelöscht werden können. Die Arbeitsgruppe hält diese Angaben im Falle von Suchmaschinen für notwendig, damit eine Verarbeitung nach Treu und Glauben gewährleistet werden kann.

In den Antworten der Suchmaschinenbetreiber auf den Fragebogen der Arbeitsgruppe finden sich bedeutende Unterschiede. Einige Suchmaschinen erfüllen die Auflagen der Richtlinie. Sie bieten sowohl auf ihrer Startseite als auch auf den bei einem Suchvorgang generierten Seiten Links zu ihren Datenschutzerklärungen und informieren über Cookies. Bei anderen Suchmaschinen gestaltet sich die Suche nach den Datenschutzerklärungen sehr schwierig. Die Benutzer müssen in der Lage sein, auf die Datenschutzerklärungen einfach zuzugreifen, bevor sie – unter anderem von der Startseite der Suchmaschine – einen Suchvorgang durchführen.

Nach den Empfehlungen der Arbeitsgruppe sollten die vollständigen Datenschutzerklärungen so umfassend und detailliert wie möglich sein und die in den Datenschutzgesetzen enthaltenen fundamentalen Grundsätze erwähnen.

Die Arbeitsgruppe weist darauf hin, dass viele Datenschutzerklärungen gewisse Mängel in Bezug auf die Auskunfts- und Löschungsrechte aufweisen, die der betroffenen Person gemäß Artikel 12, 13 und 14 der Datenschutzrichtlinie zustehen. Diese Rechte gehören zu den grundlegenden Elementen des Schutzes der Privatsphäre von Personen.

7. RECHTE DER BETROFFENEN PERSON

Die Suchmaschinen sollten die Auskunfts-, Berichtigungs- und Löschungsrechte der betroffenen Personen bezüglich sie betreffender Daten beachten. Diese Rechte gelten vor allem für die von den Suchmaschinen gespeicherten Daten von authentifizierten Benutzern, einschließlich Personenprofile. Diese Rechte gelten aber auch für nicht registrierte Benutzer, die über die Möglichkeit verfügen sollten, ihre Identität gegenüber dem Suchmaschinenbetreiber nachzuweisen, etwa durch Registrieren für den Zugriff auf künftige Daten und/oder mit einer Erklärung von ihrem Zugangsanbieter über die Verwendung einer bestimmten IP-Adresse in der Vergangenheit, über die Auskunft verlangt wird. Bei Inhaltsdaten liegt die Hauptverantwortung im Rahmen der europäischen Datenschutzgesetze generell nicht bei den Suchmaschinenbetreibern.

Die Arbeitsgruppe hat im Jahr 2000 in ihrem Arbeitspapier „Privatsphäre im Internet“²⁵ bereits folgende Erläuterungen abgegeben: „Das „Personalisieren“ von Datenprofilen setzt die vorherige Einwilligung bei Kenntnis aller Details der betroffenen Personen voraus. Sie müssen das Recht haben, ihre Zustimmung jederzeit und mit sofortiger Wirkung zu entziehen. Die Nutzer müssen jederzeit Gelegenheit haben, ihre Datenprofile zu überprüfen. Sie müssen auch das Recht haben, die gespeicherten Daten zu berichtigen oder zu löschen.“

Im konkreten Fall der Anwendung auf Suchmaschinen müssen die Benutzer das Recht haben, auf alle über sie gespeicherten personenbezogenen Daten gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zuzugreifen. Dies gilt auch für ihre bisherigen Suchvorgänge, aus anderen Quellen erfasste Daten und Daten, die ihr Verhalten oder ihre Herkunft offenbaren. Die Artikel-29-Arbeitsgruppe hält es für überaus wichtig, dass die Suchmaschinenbetreiber die notwendigen Mittel für die Ausübung dieser Rechte bereitstellen, z. B. ein webbasiertes Instrument, das registrierten Benutzern direkten Online-Zugriff auf ihre personenbezogenen Daten mit der Möglichkeit bietet, bestimmte Verarbeitungszwecke abzulehnen.

Zweitens gilt das Recht auf Berichtigung oder Löschung von Informationen auch für spezifische Daten im Cache-Speicher der Suchmaschinenbetreiber, sobald diese Daten nicht mehr mit den tatsächlichen Inhalten übereinstimmen, die im Internet von den für die Verarbeitung Verantwortlichen der Website(s) veröffentlicht werden.²⁶ In einer derartigen Situation müssen die Suchmaschinenbetreiber bei Eingang eines Antrags von einer betroffenen Person sofort reagieren und unvollständige oder veraltete Informationen entfernen oder berichtigen. Der Cache-Speicher kann durch einen automatischen, sofortigen Neubesuch der ursprünglichen Veröffentlichung aktualisiert werden. Die Suchmaschinenbetreiber sollten den Benutzern die Möglichkeit bieten, die kostenlose Entfernung derartiger Inhalte aus ihrem Cache-Speicher anzufordern.

8. SCHLUSSFOLGERUNGEN

Das Internet wurde als ein offenes globales Netzwerk für den Informationsaustausch konzipiert. Es ist jedoch notwendig, ein Gleichgewicht zwischen der Offenheit des Internet und dem Schutz der personenbezogenen Daten von Internet-Benutzern zu finden. Dieses Gleichgewicht kann durch Differenzierung zwischen den zwei verschiedenen Hauptrollen von Suchmaschinenbetreibern hergestellt werden. In ihrer ersten Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten (z. B. die IP-Adressen, die sie von Benutzern und ihrer individuellen Suchhistorie sammeln) sind sie im Rahmen der Datenschutzrichtlinie voll verantwortlich zu machen. In ihrer zweiten Rolle als Anbieter von Inhaltsdaten (z. B. den Daten im Index) liegt die Hauptverantwortung für die von ihnen verarbeiteten Daten im Rahmen der europäischen Datenschutzgesetze generell nicht bei den Suchmaschinenbetreibern. Ausnahmen sind die Verfügbarkeit eines „Langzeit-Caches“ und Mehrwert schaffende Vorgänge für personenbezogene Daten (z. B. Suchmaschinen, die Profile von natürlichen Personen erstellen). Bei der Bereitstellung derartiger Dienste tragen die Suchmaschinen im Rahmen der

²⁵ WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf

²⁶ Die Arbeitsgruppe schlägt vor, dass Herausgeber von Webseiten Maßnahmen entwickeln, um Suchmaschinen automatisch über eingegangene Anträge auf Löschung personenbezogener Daten zu informieren.

Datenschutzrichtlinie die volle Verantwortung und müssen alle einschlägigen Bestimmungen einhalten.

Gemäß Artikel 4 der Datenschutzrichtlinie gelten dessen Bestimmungen für einen für die Verarbeitung Verantwortlichen, der eine Niederlassung im Hoheitsgebiet von mindestens einem an der Verarbeitung personenbezogener Daten beteiligten Mitgliedstaat besitzt. Die Bestimmungen der Richtlinie können aber auch auf nicht im gemeinschaftlichen Hoheitsgebiet niedergelassene Suchmaschinenbetreiber anwendbar sein, wenn diese zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind.

Ausgehend von den obigen Überlegungen und unter Berücksichtigung der gegenwärtigen Vorgehensweise der Suchmaschinen können die folgenden Schlussfolgerungen gezogen werden:

Anwendbarkeit der EG-Richtlinien

- 1. Die Datenschutzrichtlinie (95/46/EG) ist grundsätzlich auf die Verarbeitung von personenbezogenen Daten durch Suchmaschinenbetreiber anwendbar, auch wenn sich deren Hauptsitz außerhalb des EWR befindet.**
- 2. Nicht im EWR ansässige Suchmaschinenbetreiber sollten ihre Benutzer darüber informieren, welche Bedingungen – Vorhandensein einer Niederlassung oder verwendete technische Mittel – sie zur Einhaltung der Datenschutzrichtlinie verpflichten.**
- 3. Die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) ist nicht auf Internet-Suchmaschinen anwendbar.**

Pflichten der Suchmaschinenbetreiber

- 4. Personenbezogene Daten dürfen von den Suchmaschinenbetreibern nur für rechtmäßige Zwecke verarbeitet werden, und die Datenmenge muss für die verschiedenen zu erfüllenden Zwecke erheblich sein und darf nicht darüber hinausgehen.**
- 5. Die Suchmaschinenbetreiber müssen personenbezogene Daten löschen oder (unumkehrbar und wirksam) anonymisieren, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr notwendig sind. Die Arbeitsgruppe fordert die Suchmaschinenbetreiber zur Entwicklung geeigneter Anonymisierungssysteme auf.**
- 6. Die Speicherungsfristen sollten auf ein Minimum reduziert werden und in einem angemessenen Verhältnis zum jeweiligen von den Suchmaschinenbetreibern angeführten Zweck stehen. Angesichts der bisher abgegebenen Stellungnahmen der Suchmaschinenbetreiber zu den möglichen Zwecken für die Erhebung personenbezogener Daten sieht die Arbeitsgruppe keine Grundlage für eine Speicherungsfrist von mehr als sechs Monaten. In den einzelstaatlichen Rechtsvorschriften kann die**

Löschung von personenbezogenen Daten jedoch bereits zu einem früheren Zeitpunkt vorgeschrieben sein. Sofern die Suchmaschinenbetreiber personenbezogene Daten länger als sechs Monate speichern, müssen sie umfassend nachweisen, dass dies für den Dienst zwingend notwendig ist. Auf jeden Fall sollte die Information über die von den Suchmaschinenbetreibern festgelegten Speicherungsfristen auf ihrer Startseite einfach zugänglich sein.

7. Auch wenn die Erhebung einiger personenbezogener Daten über die Benutzer der Dienste durch Suchmaschinenbetreiber unvermeidlich ist, wie z. B. die Erhebung der IP-Adresse aufgrund des normalen HTTP-Verkehrs, ist die Erhebung zusätzlicher personenbezogener Daten von einzelnen Benutzern nicht notwendig, um Suchergebnisse liefern und Werbeanzeigen schalten zu können.
8. Wenn die Suchmaschinenbetreiber Cookies verwenden, sollte deren Lebensdauer nicht länger als nachweisbar notwendig sein. Ähnlich wie Web-Cookies sollten Flash-Cookies nur installiert werden, wenn transparente Informationen über ihre Zweckbestimmung und die Vorgehensweise für den Zugriff auf diese Information sowie ihre Bearbeitung und Löschung mitgeteilt werden.
9. Die Suchmaschinenbetreiber müssen den Benutzern klare und verständliche Informationen über ihre Identität, ihre Niederlassung und die Daten geben, die sie zu erheben, zu speichern oder zu übermitteln beabsichtigen, sowie über deren Zweckbestimmung.²⁷
10. Die Anreicherung von Benutzerprofilen mit Daten, die nicht von den Benutzern selbst bereitgestellt werden, darf nur mit Einwilligung der Benutzer erfolgen.
11. Wenn die Suchmaschinenbetreiber Mittel zur Speicherung der individuellen Suchhistorie bereitstellen, sollten sie sich vergewissern, dass die Einwilligung des Benutzers vorliegt.
12. Die Suchmaschinenbetreiber sollten die Nichtbeteiligungsklauseln von Website-Herausgebern respektieren, die festlegen, dass die Website nicht durchsucht und indexiert oder in den Cache-Speicher der Suchmaschinen aufgenommen werden soll.
13. Wenn die Suchmaschinenbetreiber einen Cache-Speicher bereitstellen, in dem personenbezogene Daten länger als in der ursprünglichen Veröffentlichung verfügbar gemacht werden, müssen sie das Recht der betroffenen Personen respektieren, über den Zweck hinausgehende und unrichtige Daten aus dem Cache-Speicher entfernen zu lassen.

²⁷ Die Arbeitsgruppe empfiehlt ein mehrere Ebenen umfassendes Modell für die Datenschutzerklärung, so wie es in der Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten beschrieben wird
(WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_de.pdf).

14. Suchmaschinenbetreiber, die sich auf Mehrwert schaffende Vorgänge spezialisieren, wie z. B. Profilbildungsdienste für natürliche Personen (so genannte „Menschen-Suchmaschinen“) und Gesichtserkennungssoftware für Bilder, müssen einen rechtmäßigen Grund für die Verarbeitung besitzen (z. B. die Einwilligung) und alle anderen Forderungen der Datenschutzrichtlinie erfüllen, wie etwa die Verpflichtung, die Qualität der Daten und die Verarbeitung nach Treu und Glauben zu gewährleisten.

Rechte der Benutzer

15. Die Benutzer von Suchmaschinendiensten besitzen das Recht, auf alle über sie gespeicherten personenbezogenen Daten einschließlich ihrer Profile und Suchhistorie zuzugreifen und diese, falls notwendig, gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zu überprüfen und zu berichtigen.
16. Eine übergreifende Korrelation von Daten aus verschiedenen Diensten des Suchmaschinenbetreibers darf nur durchgeführt werden, wenn die Einwilligung des Benutzers für diesen speziellen Dienst vorliegt.

Brüssel, den 4. April 2008

*Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK*

ANHANG 1
BEISPIELE FÜR DIE VON SUCHMASCHINEN VERARBEITETEN DATEN
UND TERMINOLOGIE

Abfrageprotokolle	
Suchanfrage	Die in den Suchmaschinendienst eingegebene Suchanfrage, die gewöhnlich in Suchmaschinenprotokollen als URL der aufgrund der Suchanfrage angebotenen Seite gespeichert wird.
IP-Adresse	Die Internet-Protokolladresse des Computers für jede vom Benutzer eingegebene Anfrage.
Datum und Uhrzeit	Datum und Uhrzeit einer bestimmten Suchanfrage.
Cookie	Cookie(s) und/oder ähnliche auf dem Computer des Benutzers gespeicherte Objekte, einschließlich aller Cookie-Parameter, z. B. Wert und Verfallsdatum. Auf dem Server der Suchmaschine sind dies alle Daten, die sich auf das Cookie beziehen, z. B. die folgenden Informationen: „cookie/device X has been placed on computer with IP address Y, on date and time Z“ (Cookie/Objekt X wurde auf dem Computer mit der IP-Adresse Y am Datum und zur Uhrzeit Z gespeichert).
Flash-Cookie	Auch als „Local Shared Object“ bezeichnet. Ein Cookie, das mittels Flash-Technologie installiert wird. Im Gegensatz zu herkömmlichen Web-Cookies kann es derzeit nicht einfach über die Browser-Einstellungen gelöscht werden.
Referring-URL	Die URL der Website, auf der die Suchanfrage eingegeben wurde, eventuell eine URL Dritter.
Einstellungen	Mögliche benutzerspezifische Einstellungen in erweiterten Dienstumgebungen.
Browser	Einzelheiten zum Browser einschließlich des Typs und der Version.
Betriebssystem	Einzelheiten zum Betriebssystem.
Sprache	Spracheinstellungen des vom Benutzer verwendeten Browsers, aus denen sich die vom Benutzer bevorzugte Sprache ableiten lässt.
Angebotene Inhalte	
Links (Verknüpfungen)	Die Links, die einem bestimmten Benutzer aufgrund einer Anfrage zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) angeboten wurden. Die Ergebnisse der Suchmaschine sind dynamisch. Damit die Ergebnisse im Detail ausgewertet werden können, muss der Suchmaschinenbetreiber Daten über die spezifischen Links und die Reihenfolge speichern, in der die Daten zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) aufgrund einer spezifischen Benutzeranfrage angezeigt wurden.
Werbung	Die aufgrund einer bestimmten Suchanfrage angezeigte Werbung.
Benutzernavigation	Klicks durch den Benutzer auf die organischen Ergebnisse und Werbeanzeigen der Suchergebnisseite(n). Dies umfasst den Rang der spezifischen Ergebnisse, die vom Benutzer weiterverfolgt wurden (Link Nr. 1 wurde zuerst verfolgt, daraufhin kehrte der Benutzer zurück und folgte dem Link Nr. 8).
Operative Daten	Aufgrund des operativen Wertes und der Verwendung einiger der oben beschriebenen Daten (z. B. Betrugserkennung, Sicherheit/Integrität des Dienstes und Erstellung von Benutzerprofilen) werden diese Daten von den Suchmaschinen auf verschiedene Weise gekennzeichnet und analysiert. Beispielsweise kann eine bestimmte IP-Adresse als mögliche Quelle einer Anfrage oder von Klick-Spam gekennzeichnet werden; ein Klick auf eine Werbeanzeige kann als Betrug oder eine Anfrage als Verweis auf Informationsquellen zu einem bestimmten Thema gekennzeichnet werden.
Daten über registrierte Benutzer	Ein Suchmaschinenbetreiber kann den Benutzern anbieten, sich für die Nutzung von erweiterten Diensten registrieren zu lassen. Der Betreiber verarbeitet typischerweise Benutzerkontodaten, wie beispielsweise die Anmelde- und Kennwortdaten des Benutzers, eine Adresse für elektronische

	Post und andere vom Benutzer angegebene, personenbezogene Daten wie Interessen, Vorlieben, Alter und Geschlecht.
Daten anderer Dienste/Quellen	Die meisten Suchmaschinenbetreiber bieten zusätzliche Dienste wie elektronische Post, Desktop-Suche und Werbung auf Websites sowie für die Dienste Dritter an. Diese Dienste erzeugen Benutzerdaten, die korreliert und verwendet werden können, um das vorhandene Wissen über die Benutzer der Suchmaschine zu erweitern. Die Benutzerdaten und möglichen Profile können auch mit Daten aus anderen Quellen angereichert werden, z. B. mit Geolokationsdaten von IP-Adressen und demografischen Daten.

ANHANG 2

FRAGEBOGEN FÜR SUCHMASCHINENBETREIBER ZUR DATENSCHUTZERKLÄRUNG

1. Speichern Sie Daten über die individuelle Nutzung Ihrer Suchdienste?
2. Welche Art von Informationen speichern/archivieren Sie im Zusammenhang mit Ihren Suchdiensten? (z. B. Server-Protokolle, Schlüsselwörter, Suchergebnisse, IP-Adressen, Cookies, Klickdaten, Momentaufnahmen von Websites (Caches) usw.)
3. Fordern Sie die Einwilligung (freie Willenserklärung) des Benutzers bei der Speicherung der Daten an, die Sie in Ihrer Antwort auf Frage 2 genannt haben? Falls ja, wie fordern Sie sie an? Falls nein, auf welcher Rechtsgrundlage begründen Sie die Speicherung dieser Daten?
4. Erstellen Sie Profile über das Benutzerverhalten auf Basis der Daten, die Sie in Ihrer Antwort auf Frage 2 angegeben haben? Falls ja, für welche Zwecke? Welche Daten verarbeiten Sie? Unter welcher Kennung (z. B. IP-Adresse, Benutzerkennung, Cookie-ID) speichern Sie Profile? Fordern Sie die Einwilligung des Benutzers an?
5. Falls Sie zusätzlich zu den Suchdiensten andere personalisierte Dienste anbieten: Nutzen Sie die im Rahmen Ihrer Suchdienste erhobenen Daten gemeinsam mit diesen anderen Diensten und/oder umgekehrt? Falls ja, geben Sie bitte an, welche Daten dies betrifft.
6. Wie lange speichern Sie die Daten, die Sie in Ihrer Antwort auf Frage 2 angegeben haben, und für welche Zwecke?
7. Welche Kriterien sind bei der Festlegung der Speicherungsfrist für Sie maßgeblich?
8. Falls Sie Daten über einen befristeten Zeitraum speichern: Was tun Sie nach Ablauf dieser Frist, und welche diesbezüglichen Verfahren sind vorhanden?
9. Anonymisieren Sie Daten? Falls ja: Wie anonymisieren Sie die Daten? Ist die Anonymisierung unumkehrbar? Welche Informationen sind in den anonymisierten Daten immer noch enthalten?
10. Bestehen Zugriffsmöglichkeiten auf die Daten, z. B. für Personal, oder werden sie ohne menschliche Eingriffe verarbeitet?

11. Geben Sie Daten an Dritte weiter? In welchen Ländern? Geben Sie bitte für die folgenden Kategorien an, welche Arten von Daten Sie eventuell weitergeben und in welchen Ländern dies der Fall ist:
- Werbetreibende
 - Werbepartner
 - Strafverfolgungsbehörden (Einhaltung rechtlicher Verpflichtungen zur Offenlegung der Daten, beispielsweise vor Gericht)
 - Sonstige (bitte angeben):
12. Wie informieren Sie die Benutzer über die Datenerhebung, Datenverarbeitung und Datenspeicherung? Geben Sie den Benutzern umfassende Informationen, z. B. über Cookies, Profilbildung und sonstige Werkzeuge, die die Aktivitäten auf der Website überwachen? Falls ja, fügen Sie bitte eine Kopie der Informationshinweise sowie eine Beschreibung ihrer Anordnung an.
13. Geben Sie den Benutzern die Möglichkeit, das Zugangsrecht und das Recht auf Berichtigung, Änderung, Löschung oder Sperrung der Daten auszuüben? Besteht die Möglichkeit, sich der Datenerhebung oder -speicherung vollständig zu entziehen („Opt-out“), so dass keine personenbezogenen Daten erhoben werden und der Benutzer keinerlei Spuren auf einem relevanten Speichersystem hinterlässt? Ist die Ausübung dieser Rechte mit Kosten verbunden?
14. Wenden Sie Sicherheitsmaßnahmen auf die Datenspeicherung an? Welche?
15. Haben Sie sich mit einer nationalen Datenschutzbehörde im EWR in Verbindung gesetzt? Falls ja, geben Sie bitte die Behörde an. Falls nein, geben Sie bitte die Gründe an, weshalb Sie dies bisher unterlassen haben.