ARTIKEL-29-DATENSCHUTZGRUPPE

10092/05/DE
WP 104

Arbeitspapier

Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten

18. Januar 2005

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges EU-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, Generaldirektion Binnenmarkt und Dienstleistungen, Referat D4 (Wissensbestimmte Wirtschaft - Datenschutz), B-1049 Brüssel, Belgien, Büro C100-6/136.

Website: www.europa.eu.int/comm/privacy

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 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

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

HAT DIESES ARBEITSPAPIER ANGENOMMEN ZUM THEMA:

Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten

I. Hintergrund

Die Datenschutzgruppe stellt fest, dass der aufgrund der Entwicklung des Internet zunehmende Informationsaustausch immer stärker die heikle Frage der Kontrolle über die Nutzung urheberrechtlich geschützten Materials berührt. Dabei geht es insbesondere um die Rechte und Pflichten von Akteuren, die ein Interesse an urheberrechtlich geschütztem Material haben und mit der Verwaltung digitaler Rechte befasst sind.

Die Datenschutzgruppe weiß einerseits um die Notwendigkeit von Maßnahmen, mit denen die berechtigten Interessen der Inhaber von Immaterialgüterrechten (Rechte des geistigen Eigentums) vor mutmaßlichem Betrug geschützt werden können. Andererseits hat die Datenschutzgruppe festgestellt, dass einige dieser Maßnahmen, die von den Urheberrechtsinhabern auf verschiedenen Ebenen ergriffen wurden, um den unrechtmäßigen Austausch urheberrechtlich geschützten Materials wirksam zu verhindern, die Verarbeitung personenbezogener Daten beinhalten. Zuerst möchte sich die Datenschutzgruppe mit der digitalen Rechteverwaltung (*Digital Rights Management – DRM*) befassen, die sich derzeit entwickelt; dabei geht es ihr konkret darum, dass DRM die Identifizierung und Nachverfolgung von Einzelpersonen ermöglichen, die über das Internet auf gesetzlich geschütztes Material zugreifen (zum Beispiel auf Musikaufnahmen oder Software). Anschließend geht die Datenschutzgruppe auf die Möglichkeiten der Urheberrechtsinhaber ein, ihre Rechte gegenüber Einzelpersonen durchzusetzen, die im Verdacht der Urheberrechtsverletzung stehen.

Dieses Papier beleuchtet die unterschiedlichen Niveaus, auf denen sich Datenschutzfragen ergeben; es fasst die wesentlichen Rechtsgrundsätze zusammen, die nicht nur von den Urheberrechtsinhabern bei der Ausübung ihrer Rechte zu beachten sind, sondern auch von anderen Akteuren, die in besonderer Weise mit der digitalen Rechteverwaltung zu tun haben, beispielsweise die betroffenen Wirtschaftszweige und Dienstanbieter, die Technologie zur digitalen Rechteverwaltung anbieten.

a. Digitale Rechteverwaltung

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

Zur Entwicklung der digitalen Rechteverwaltung merkt die Datenschutzgruppe an, dass sich neue Technologien zur Identifizierung und/oder Nachverfolgung von Benutzern sowohl auf der Informationsaustauschebene als auch auf der Plattformebene durchsetzen (d. h. Überprüfung von Hardware/Software).

Beim Austausch bzw. Herunterladen urheberrechtlich geschützten Materials im Internet wird der Zugang zu diesem Material immer häufiger von einer vorherigen Überprüfung der Identität des Benutzers abhängig gemacht; außerdem wird die Nutzung des Materials anschließend mittels Etiketten (*tags*) oder digitalen Wasserzeichen weiterverfolgt. Beispiel: Ein Benutzer muss sich häufig identifizieren, bevor er ein Musikstück eines offiziellen Anbieters herunterladen kann; sein Profil wird dabei um Informationen aus der eindeutigen Kennung ergänzt, die in jedem heruntergeladenen Musikstück enthalten ist. Neben dem erklärten Zweck der Kontrolle der individuellen Nutzung des Materials im Einklang mit DRM wird die Kennzeichnung oft auch zur Erstellung von Benutzerprofilen und zur gezielten Werbung verwendet. Die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation stellte dazu fest: „Elektronische Copyright-Management-Systeme (ECMS), die zur allgegenwärtigen Überwachung von Nutzern digitaler Werke führen könnten, werden entwickelt und angeboten. Einige ECMS überwachen jede einzelne Handlung des Lesens, Anhörens und Betrachtens im Internet durch individuelle Nutzer, wobei hoch sensible Informationen über die Betroffenen gesammelt werden“[2].

Auf der Plattformebene verfolgt die Datenschutzgruppe bereits eingehend die Entwicklung einiger Industrieprojekte, z. B. TCG, die darauf abstellen, die Vertrauenswürdigkeit von Informationen zu gewährleisten, die in einer Computerplattform enthalten sind bzw. auf die von einer Computerplattform aus zugegriffen wird. Wenngleich solche Systeme sich sehr positiv auf den Grad der Informationssicherheit auswirken können, was die Datenschutzgruppe bereits eingeräumt hat, so sind deren Anwendungsmöglichkeiten doch sehr vielfältig. Die Bestandteile von Computerplattformen könnten durchaus von außen auf die Beachtung von Urheberrechten hin überprüft werden. Die Datenschutzgruppe hat in ihrem Arbeitspapier WP 86 vom 23. Januar 2004 bereits darauf hingewiesen, dass TPM-basierte Anwendungen z. B. auch von der Contentindustrie eingesetzt werden könnten, „um die Kontrolle über Verbreitung und Nutzung von digitalem Content (einschließlich Software) zurückzugewinnen, die sie mit dem Aufkommen von Internet und Peer-to-Peer-Anwendungen verloren hat“. Derartige Kontrollen könnten bei jeder Kontaktaufnahme zwischen Plattformen routinemäßig erfolgen, denn „der von einer derart starken Vertretung der Industrie propagierte TPM-Einsatz dürfte zum De-facto-Standard werden, zu einer notwendigen Voraussetzung für die Teilhabe an der Informationsgesellschaft“.

b. Durchsetzung von Urheberrechten

Einerseits wird an der Quelle auf Kontrolle und Nachverfolgung gesetzt in dem Bestreben, jeden Benutzer, der Material rechtmäßig aus dem Internet herunterlädt, „im Vorfeld“ zu überprüfen; andererseits führt der Urheberrechtsschutz dazu, dass die meisten betroffenen Akteure auch Maßnahmen „im Nachfeld“ ergreifen und Ermittlungen gegen mutmaßliche Rechtsverletzer durchführen.

Die Rechteinhaber setzen dabei unterschiedliche Instrumente ein; die Folgenden möchte die Datenschutzgruppe besonders hervorheben:

Häufig wird auf Internet-gestützte Peer-to-Peer-Instrumente zurückgegriffen, um Informationen über Einzelpersonen zu gewinnen, die geschütztes Material online bereitstellen oder herunterladen.

[2] Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: „Gemeinsamer Standpunkt - Datenschutz und Urheberrechts-Management“, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000.

Die Rechteinhaber erfassen bei ihren Recherchen in der Regel die IP-Adressen der Benutzer[3]. Diese Informationen werden dann mit den Benutzerdaten der Internetdienstanbieter (*ISP*) verknüpft. In manchen Fällen verlangen die Rechteinhaber von den Internetdienstanbietern direkt die Preisgabe der Benutzeridentität, um die Benutzer schriftlich abzumahnen. In anderen Fällen fordern die Rechteinhaber die Internetdienstanbieter auf, die betreffenden Benutzer schriftlich zur Entfernung des mutmaßlich rechtsverletzenden Materials aufzufordern oder ihnen den Netzzugang zu sperren.

In welchem Umfang Rechteinhaber Zugang zu detaillierten Benutzerinformationen erhalten, ist von Land zu Land unterschiedlich. In Belgien fordern die Rechteinhaber die Internetdienstanbieter auf, Warnungen an die Benutzer zu richten. In den Vereinigten Staaten wurden die Internetdienstanbieter aufgefordert, der Musikindustrie die Identität ihrer Kunden ohne richterliche Anordnung *direkt* mitzuteilen[4]. In anschließenden Gerichtsentscheidungen (siehe Rechtssache Verizon vom Dezember 2003) stellten die Gerichte allerdings fest, dass die direkte Übermittlung von Daten an Rechteinhaber als rechtswidrig anzusehen ist. Ein anderes Beispiel liefert das australische Recht mit der als „*Anton Piller Order*" bekannten Verfügung; diese ermöglicht die Erhebung von Beweismitteln, einschließlich Hausdurchsuchungen, durch private Akteure, beispielsweise die Inhaber von Immaterialgüterrechten.

Um mutmaßliche Rechtsverletzungen auf die verantwortlichen Benutzer zurückführen und die Profile der Benutzer ergänzen zu können, versuchen die Rechteinhaber, bestehende öffentliche Register wie „Whois"-Datenbanken zu nutzen, in denen Angaben zu Personen gespeichert sind, die einen Domainnamen haben registrieren lassen. Sie enthalten vornehmlich Informationen über den dem Domainnamen zugehörigen Ansprechpartner, darunter Name, Telefonnummer, E-Mail-Adresse und sonstige personenbezogene Daten. Auf einige Angaben kann direkt online zugegriffen werden, andere sind offline gespeichert und müssen somit bei der für die Datenbank verantwortlichen Stelle abgerufen werden.

Schließlich sei noch Folgendes angemerkt: Die Erhebung personenbezogener Daten durch Rechteinhaber ist an bestimmte Datenschutzgrundsätze gebunden; vor diesem Hintergrund stellt die Datenschutzgruppe fest, dass Erörterungen mit Interessenträgern in mehreren Ländern im Gange sind, die darauf abzielen, ihnen mehr Spielraum bei der Verarbeitung personenbezogener Daten einzuräumen. So enthält das französische Datenschutzgesetz beispielsweise jetzt eine Ausnahmeregelung, die einigen gesetzlich bestimmten[5] Rechteinhabern erlaubt, unter gewissen Voraussetzungen und mit vorheriger Genehmigung der französischen Datenschutzbehörde[6] Strafverfolgungsdaten zu verarbeiten.

---

[3] Noch vor wenigen Jahren wurden vielen Benutzern dynamische Adressen zugewiesenen, die sich beim Aufbau einer Internetverbindung stets änderten. Kabelanschlüsse und ADSL bringen mit sich, dass den Benutzern permanente IP-Adressen zugewiesen werden. Permanente IP-Adressen, die mit dem neuen Internetprotokoll IPv6 zum Standard werden könnten, machen die Nachverfolgung von Internetnutzern noch einfacher (siehe dazu die Stellungnahme 2/2002 der Datenschutzgruppe vom 30. Mai 2002: „Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6", 10750/02/DE, WP 58).

[4] Dabei beriefen sich die Rechteinhaber auf *Section 512* der *Digital Millennium Copyright Act* bezüglich Haftungseinschränkungen im Zusammenhang mit Online-Material. Diese Vorschriften ermöglichen es einem Urheberrechtsinhaber oder seinem Vertreter, bei einem Bundesgericht eine Verfügung gegen einen Internetdienstanbieter zu erwirken, der dann die Identität eines Benutzers preisgeben muss, der urheberrechtsverletzender Handlungen verdächtigt wird. Dieses Verfahren ist recht flexibel, da auf diesem Wege personenbezogene Daten des Benutzers beschafft werden können, ohne ein ordentliches Gerichtsverfahren einleiten zu müssen.

[5] Die Ausnahme gilt für die in Artikel L 321-1 und L 331-1 des Urheberrechtsgesetzes erschöpfend aufgeführten Rechtspersönlichkeiten und dient dem Interessenschutz der Rechteinhaber.

[6] Die Nationale Kommission für Informatik und Freiheiten (*CNIL*) hat die Art der in den Dateien enthaltenen Strafverfolgungsdaten sowie deren Speicherfrist genauer auszuführen. Ferner muss sie sicherstellen, dass eine derartige Verarbeitung angemessen ist und nicht über das zur Bekämpfung betrügerischer Nachahmung unbedingt nötige Maß

Die Datenschutzgruppe muss in diesem sich wandelnden Kontext an die wesentlichen Datenschutzgrundsätze erinnern und darlegen, in welchem Maße sie für die digitale Rechteverwaltung und die Durchsetzung von Urheberrechten gelten.

II. Die Verwaltung von Immaterialgüterrechten

Wenn Rechteinhaber den berechtigten Zweck verfolgen, den Missbrauch urheberrechtlich geschützten Materials zu verhindern, bringt dies häufig die Nachverfolgung von Benutzern und die Überwachung ihrer Präferenzen mit sich. Vor allem die Verwendung eindeutiger Kennungen in Verbindung mit den gesammelten personenbezogenen Daten mündet in die Verarbeitung detaillierter personenbezogener Daten. Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten stellten mehrere Grundsätze auf, die von einem Rechteinhaber beachtet werden müssen, wenn personenbezogene Daten verarbeitet werden. Artikel 2 Absatz 3 Buchstabe a der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums verweist darauf, dass sie die Richtlinie 95/46/EG nicht berührt und folglich die Datenschutzgrundsätze zu beachten sind.

Dieses Papier konzentriert sich auf den Grundsatz der Notwendigkeit, ferner auf die Notwendigkeit des anonymen Zugangs zu Netzdiensten, auf den Grundsatz der Transparenz, die Vereinbarkeit der Zweckbestimmungen und die Beschränkungen hinsichtlich der Speicherung von Daten.

- Grundsätze der Notwendigkeit und der Anonymität

Die Datenschutzgruppe bekräftigt erneut die Notwendigkeit, Transaktionen im Internet anonym oder pseudonym durchführen zu können. Diesen Grundsatz hat die Datenschutzgruppe mehrfach ausgeführt[7], erstmalig in ihrer Empfehlung vom 3. Dezember 1997, worin die Datenschutzgruppe bereits feststellte, dass die Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten im Internet ebenso einzuhalten seien wie bei der Offline-Verarbeitung. Auch die Internationale Arbeitsgruppe vertritt die Ansicht, „dass die Nutzer generell die Möglichkeit haben sollten, auf das Internet ohne Preisgabe ihrer Identität zuzugreifen, sofern personenbezogene Daten nicht für die Erbringung eines bestimmten Dienstes erforderlich sind“[8]. Dieser Grundsatz wird von dem Notwendigkeitsgrundsatz in Artikel 6 Buchstabe c der Datenschutzrichtlinie untermauert; danach muss sichergestellt werden, dass die personenbezogenen Daten „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“.

Diesbezüglich betont die Datenschutzgruppe, dass bei der Verwendung von DRM-Technologien zum Schutz eines bestimmten Materials Instrumente eingesetzt werden sollten, die die Anonymität des Benutzers wahren. Daher sollten datenschutzfreundliche Technologien bei der Entwicklung dieser neuen Instrumente größere Beachtung finden.

- Verwendung eindeutiger Kennungen

---

hinausgeht (Entscheidung des „Verfassungsrats“ Nr. *2004-499 DC, 29. Juli 2004*). Der Verfassungsrat vertritt übrigens die Auffassung, dass das Identifizieren von Benutzern mittels ihrer IP-Adresse nur im Rahmen eines gerichtlichen Verfahrens zulässig ist.

[7] Empfehlung 3/97 „Anonymität auf dem Internet“, angenommen am 3.12.1997, WP 6;
Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet, angenommen am 23. Februar 1999, 5013/99/DE/endg., WP 16;
Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware, angenommen am 23. Februar 1999, 5093/98/DE/endg., WP 17;

[8] Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation, a.a.O., S. 2.

Die Verwendung eindeutiger Kennungen ermöglicht die Verknüpfung von Daten zu einer bestimmten Person und erleichtert das Erstellen von Profilen. Bei der digitalen Rechteverwaltung ermöglichen diese Kennungen die Erstellung von Benutzerprofilen anhand von Art und Menge des abgerufenen Materials. Beispiel: Ein Anbieter von Rechtsinhalten kann den Weg von Dateien, die ein digitales Wasserzeichen in Form einer eindeutigen Kennung tragen, innerhalb von Peer-to-Peer-Netzen verfolgen und den Benutzer ausfindig machen, der das Material ursprünglich rechtmäßig heruntergeladen und gegebenenfalls anschließend mutmaßlich rechtswidrig weiterverwendet hat. Auch am Arbeitsplatz hätte die Musik- oder Filmwirtschaft die Möglichkeit, die Benutzung des angebotenen urheberrechtlich geschützten Materials durch ihre Mitarbeiter nachzuverfolgen. Die Datenschutzgruppe stellt die Nutzung von Kennungen ernstlich in Frage, die der Verfolgung aller Benutzer im Vorfeld dient und darauf abstellt, im Falle eines mutmaßlichen Urheberrechtsmissbrauchs eine bestimmte Person herauszufiltern. Die Etikettierung von Material sollte nicht mit der Identität einer Einzelperson verknüpft werden, es sei denn, die Verknüpfung ist zur Erbringung der Dienstleistung erforderlich oder die Einzelperson wurde darüber informiert und hat dem zugestimmt.

- Information des Betroffenen

Wie die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation betont hat, sollte für größtmögliche Transparenz beim Betrieb der Copyright-Management-Systeme gesorgt werden. Gemäß Artikel 10 der Richtlinie 95/46/EG dürfen personenbezogene Daten nur dann erhoben werden, wenn der betroffenen Person bestimmte Auskünfte erteilt werden, dazu zählen vornehmlich die Identität des für die Verarbeitung Verantwortlichen, der Verarbeitungszweck, die Empfänger oder Empfängerkategorien der Daten sowie das Bestehen von Auskunfts- und Berichtigungsrechten.

Diese Informationen sollten gut sichtbar angezeigt werden, bevor der Benutzer personenbezogene Daten bereitstellt oder gekennzeichnetes Material herunterlädt[9].

- Zweckbindungsgrundsatz (Vereinbarkeit)

Personenbezogene Daten, die beim Benutzer auf freiwilliger Basis erhoben wurden oder die zur Erbringung der Dienstleistung erforderlich sind, sollten grundsätzlich nur zum angegebenen Zweck verwendet werden, so wie es in Artikel 6 Absatz 1 Buchstabe b der Richtlinie ausgeführt wird. Beispiel: Bei einer Kreditkartentransaktion ist es nicht zulässig, Name und Adresse des Benutzers zu erfassen, um die Daten anschließend für das Direktmarketing zu verwenden, nachdem sie mit Benutzerpräferenzen verknüpft wurden, die aus heruntergeladenem, digital gekennzeichnetem Material gewonnen wurden. Auch gemäß Artikel 13 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sind derartige Profile und die Vermarktung personenbezogener Daten nur bei vorheriger Einwilligung der Betroffenen gestattet. Derselbe Grundsatz gilt auch für die etwaige Übermittlung der personenbezogenen Daten an Dritte. Die Datenschutzgruppe unterstreicht ferner, dass die Sammlung von Daten über Konsumgewohnheiten die Verarbeitung sensibler Daten nach sich ziehen kann, wenn Benutzerprofile aus der Art der abgerufenen Informationen zusammengestellt werden (z. B. beim Herunterladen eines Buches über religiöse oder politische Fragen). Eine derartige Verarbeitung darf nur unter strenger Einhaltung der Bestimmungen von Artikel 8 der Richtlinie 95/46/EG erfolgen.

[9] Siehe Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, angenommen am 17. Mai 2001, 5020/01/DE/endg, WP 43.

- Befristete Speicherung personenbezogener Daten

Gemäß Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG müssen personenbezogene Daten in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Alle personenbezogenen Daten, die bei der Lieferung urheberrechtlich geschützten Materials oder bei der Erbringung einer urheberrechtlich geschützten Dienstleistung erfasst wurden, müssen daher unverzüglich gelöscht werden, sobald der Bedarfszweck entfallen ist, dieser Bedarfszweck kann die Rechnungsstellung sein oder die Erfüllung eines Zwecks, in den der Benutzer eingewilligt hat, z. B. die Pflege einer Geschäftsbeziehung. Es wäre mit diesem Rechtsgrundsatz unvereinbar, wenn grundsätzlich alle Benutzerdaten gespeichert würden, weil die Möglichkeit besteht, dass ein bestimmter Benutzer urheberrechtlich geschütztes Material missbräuchlich verwendet.

III. Ausmaß der Ermittlungsbefugnisse

Abgesehen von der Entwicklung technischer Schutzvorkehrungen, die auf die Etikettierung und die Nachverfolgung urheberrechtlich geschützten Materials abstellen, leiten Urheberrechtsinhaber seit einigen Jahren auch konkrete rechtliche Schritte gegen mutmaßliche Urheberrechtsverletzer ein. Dazu müssen - wie in Abschnitt I b dargelegt - Daten über Verdächtige gesammelt werden, was mit unterschiedlichen Mitteln und unter Verwertung unterschiedlicher öffentlich oder nicht öffentlich zugänglicher Quellen geschehen kann.

Zwar ist eine derartige Verarbeitung von Daten zweifellos rechtlich zulässig, wenn sie im Rahmen eines eigenen Rechtsstreits erfolgt, die Verfahren zur Datensammlung und die Art der erfassten Daten unterliegen aber datenschutzrechtlichen Regelungen; diesbezüglich sind folgende Grundsätze zu beachten:

- Grundsatz der Vereinbarkeit

Rechteinhaber konzentrieren sich bei ihren Nachforschungen in erster Linie auf online gewinnbare Fakten, z. B. die Darstellung urheberrechtlich geschützten Materials in Peer-to-Peer-Netzen. Auf Angaben wie das Datum und die Uhrzeit einer etwaigen Rechtsverletzung, die Art des geschützten Materials und auf indirekte Identifikationsmerkmale, z. B. Pseudonyme des möglichen Rechtsverletzers, lässt sich zugreifen. Somit ist die Versuchung groß, diese Sammlung personenbezogener Daten um weitere Angaben zu ergänzen, die sich unter Mithilfe des Internet-Dienstanbieters oder aus anderen Datenbanken, z. B. den Whois-Datenbanken mit Angaben über die Inhaber von Domänennamen, gewinnen lassen.

Die Datenschutzgruppe weist nachdrücklich auf die rechtlichen Beschränkungen hin, denen die Weiterverwendung personenbezogener Daten unterliegt. Der Inhalt von Datenbanken darf - unabhängig davon, ob sie öffentlich und nicht öffentlich sind, - nur für Zwecke verarbeitet und weiterverwendet werden, die mit der ursprünglichen Zweckbestimmung vereinbar sind. Zur Whois-Datenbank stellte die Datenschutzgruppe bereits in ihrer Stellungnahme vom 13. Juni 2002[10] fest: „Aus dem Blickwinkel des Datenschutzes muss unbedingt klar festgelegt werden, was die eigentliche Zweckbestimmung von Whois ist und welche Zwecke als rechtmäßig anzusehen sind und als mit der eigentlichen Zweckbestimmung vereinbar. […] Dies ist eine

[10] Stellungnahme 2/2003 zur Anwendung der Datenschutzgrundsätze auf die Whois-Verzeichnisse, 10972/03/DE endg., WP 76.

außerordentlich heikle Angelegenheit, da es nicht angehen kann, dass die Zweckbestimmung der Whois-Verzeichnisse einfach nur deshalb auf andere Zwecke ausgedehnt wird, weil dies von einigen potenziellen Benutzern der Verzeichnisse als wünschenswert angesehen wird. Einige Zwecke, die Datenschutzprobleme (Vereinbarkeit) hervorrufen könnten, sind beispielsweise die Nutzung der Daten durch privatwirtschaftliche Akteure bei der Selbstkontrolle im Zusammenhang mit mutmaßlichen Verstößen gegen ihre Rechte, z. B. auf dem Gebiet der Verwaltung digitaler Rechte (Digital Rights Management).“

Der Vereinbarkeitsgrundsatz und die Beachtung des Vertraulichkeitsgrundsatzes der Richtlinien 2002/58/EG und 95/46/EG verbieten, dass Datenbestände der Internetdienstanbieter, die zu bestimmten Zwecken verarbeitet werden und im Wesentlichen auch die Leistung eines Telekommunikationsdienstes betreffen, an Dritte weiterübermittelt werden, z. B. an Rechteinhaber; davon ausgenommen sind unter klaren gesetzlichen Voraussetzungen die Strafverfolgungsbehörden.

- Aufgaben der Internetdienstanbieter

Die Datenschutzgruppe erinnert daran, dass die Internetdienstanbieter gemäß Artikel 15 der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr nicht systematisch zur Überwachung oder Zusammenarbeit verpflichtet sind.
Internetdienstanbieter müssen außerdem nur in bestimmten Fällen, in denen eine Verfügung der Strafverfolgungsbehörden vorliegt, für eine generelle vorherige Speicherung urheberrechtlich relevanter Verkehrsdaten sorgen. Dazu stellte die Datenschutzgruppe mehrfach[11] fest: „Wenn in besonderen Fällen Verkehrsdaten aufbewahrt werden sollen, muss eine beweisbare Notwendigkeit vorliegen und die Zeitdauer der Aufbewahrung muss so kurz wie möglich sein; weiterhin muss die diesbezügliche Praxis gesetzlich in einer Weise klar geregelt sein, die ausreichenden Schutz gegen unrechtmäßigen Zugang und anderweitigen Missbrauch bietet.“

- Verarbeitung von Strafverfolgungsdaten

Gemäß Artikel 8 Absatz 5 der Datenschutzrichtlinie darf die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, nur unter strengen, von den Mitgliedstaaten festgelegten Voraussetzungen erfolgen. Wenngleich dem Einzelnen zweifelsohne das Recht zusteht, Strafverfolgungsdaten im Rahmen eines eigenen Rechtsstreits zu verarbeiten, so geht der Grundsatz doch nicht so weit, dass er die gründliche Ermittlung, Erfassung und Zentralisierung personenbezogener Daten durch Dritte erlauben würde, wozu auch generelle systematische Ermittlungen wie das Durchforsten des Internet (Internet-Scanning) zählen oder die Anforderung personenbezogener Daten aus den Beständen anderer Akteure, z. B. Internetdienstanbieter oder Stellen, die für die Verarbeitung von Wohis-Verzeichnissen verantwortlich sind. Derartige Ermittlungen sind Sache der Strafverfolgungsbehörden.

Diesbezüglich stellt die Datenschutzgruppe fest, dass die kürzlich verabschiedete Richtlinie 2004/48/EG vom 28. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums Bedingungen nennt, unter denen personenbezogene Daten von den Strafverfolgungsbehörden angefordert werden. Diese Behörden können auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag hin anordnen, dass Auskünfte über den Ursprung und die Vertriebswege von immaterialgüterrechtsverletzenden Waren oder Dienstleistungen erteilt werden, wenn die

[11] Vgl. Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.-11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation, angenommen am 11. Oktober 2002, 11818/02/DE/endg., WP 64.

Rechtsverletzung in gewerblichem Ausmaß erfolgte und wenn dabei die Grundsätze beachtet werden, die die Vertraulichkeit der Informationsquellen oder die Verarbeitung personenbezogener Daten betreffen. Es gilt, einen gerechten Ausgleich zwischen den legitimen Interessen der betroffenen Urheberrechtsinhaber und Einzelpersonen zu finden. Das Kriterium des wirtschaftlichen Vorteils aus der Rechtsverletzung kann in dieser Hinsicht entscheidend sein.

4. Fazit

Die Datenschutzgruppe stellt mit Besorgnis fest, dass die rechtmäßige Nutzung von Technologien zum Schutz urheberrechtlich geschützter Werke den Schutz personenbezogener Daten beeinträchtigen könnte. Die Anwendung der Datenschutzgrundsätze auf die digitale Rechteverwaltung lässt erkennen, dass der Schutz des Einzelnen in der Offline-Welt und der Schutz des Einzelnen in der Online-Welt immer stärker auseinanderklaffen, besonders vor dem Hintergrund genereller Nachverfolgung und Profilerstellung. Die Datenschutzgruppe fordert die Entwicklung datenschutzgerechter technischer Instrumente, und ganz allgemein die transparente und begrenzte Nutzung eindeutiger Kennungen, die dem Benutzer eine Wahlmöglichkeit zugestehen.

Im Hinblick auf die Ermittlungsbefugnisse muss die Datenschutzgruppe daran erinnern, dass sich private Akteure, z. B. Urheberrechtsinhaber, bei Ermittlungen wie oben erläutert in einem klaren Rechtsrahmen bewegen müssen; dies gilt in besonderem Maße für die Frage, welche Informationen rechtmäßig erfasst werden dürfen und welche Durchsetzungsbefugnisse diesen Akteuren eingeräumt werden können.

Brüssel, den 18. Januar 2005
Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR