EUROPÄISCHE KOMMISSION
GENERALDIREKTION XV
BINNENMARKT UND FINANZDIENSTLEISTUNGEN
Freier Verkehr von Informationen; Gesellschaftsrecht und finanzielle Information
Freier Verkehr von Informationen, Datenschutz und damit zusammenhängende internationale Aspekte

XV D/5022/97 endg. DE
WP 6

Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten

EMPFEHLUNG 3/97

Anonymität im Internet

Von der Arbeitsgruppe am 3. Dezember 1997 angenommene Diskussionsgrundlage

**ARBEITSGRUPPE FÜR DEN SCHUTZ VON PERSONEN
BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN**

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und 30 Absatz 3 dieser Richtlinie,

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

hat folgende Empfehlung verabschiedet:

Nach Verabschiedung der Diskussionsgrundlage XV/5022 (Anonymität im Internet) und Kenntnisnahme des Report and Guidance der Internationalen Arbeitsgruppe über Datenschutz im Telekommunikationswesen ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet") auf ihrer achten Sitzung in Brüssel vom 3. Dezember 1997

empfiehlt die Arbeitsgruppe, daß die Europäische Kommission anhand des beigefügten Diskussionspapiers (Anonymität im Internet, Anhang 1) sowie der Empfehlungen des Budapest-Berlin Memorandums (Anhang 2) Vorschläge entwickelt, um ihre Verwirklichung durch die geeigneten internationalen Foren zu unterstützen.

1 ABl. Nr. L 281 vom 23.11.1995, S. 31.

Diskussionsgrundlage - Anonymität im Internet

Auf der 8. Sitzung angenommen

Einführung

Die rasche Entwicklung von Internet und die starke Zunahme der über dieses neue Medium verfügbaren Arten und Anzahl von Diensten sind gut belegt. Eindeutig bedeutet das Internet-Phänomen bereits einen Wandel für unsere Lebens- und Arbeitsweise als Erwerbstätige und Bürger durch die ungeheueren Veränderungen für die Art und Weise, in der Güter und Dienste erworben und angeboten werden, und durch die Verhaltensumbildung von Organisationen im öffentlichen und im privaten Bereich.

Für diejenigen, die bei dem Prozeß der Festlegung, Entwicklung und Ausführung der öffentlichen Politik mitwirken, bedeuten derart dramatische und weitreichende Veränderungen unvermeidbar neue Probleme und neue Herausforderungen. Anfänglich lag der Schwerpunkt der politischen Planung auf dem Potential von Internet als einem Forum für kriminelles oder unerwünschtes Online-Verhalten (Vertrieb von Kinderpornographie) wie auch einem "sicheren" Kommunikationsmittel zur Erleichterung krimineller Offline-Tätigkeiten.

Auf europäischer Ebene waren diese Belange der Hauptbeweggrund für eine Reihe von Initiativen: das Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten (KOM(96)483 endg.), die Mitteilung der Kommission über illegale und schädigende Inhalte im Internet (KOM(96)487), die Entschließung des Rates vom 28. November 1996 über illegale und schädigende Inhalte und der Bericht der Arbeitsgruppe über illegale und schädigende Inhalte, der von der informellen Ratstagung in Bologna erstellt wurde.

Allmählich stellte sich jedoch heraus, daß noch viele andere Themenkreise betroffen sind. Die Mitteilung der Kommission "Europäische Initiative für den elektronischen Geschäftsverkehr" (KOM(97)157) versucht, eine Reihe weiterer wichtiger Politikbereiche in die Debatte einzubeziehen, wie die Besteuerung (insbesondere die MwSt.) auf den Online-Geschäftsverkehr und den Schutz für Rechte am geistigen Eigentum in bezug auf Inhalte, die im Online-Bereich verbreitet werden.[2]

In allen diesen Bereichen werden neue Ideen erörtert und neue potentielle Lösungen vorgeschlagen, die sicherstellen sollen, daß die über Jahrzehnte hinweg entwickelten herkömmlichen Werte und gesellschaftlichen Belange in diesem neuen technologischen Zeitalter bewahrt werden können. Ein Problem, das sich in vielen dieser Bereiche stellt, ist die Schwierigkeit festzustellen, daß tatsächlich eine rechtswidrige Tätigkeit stattgefunden hat, und sodann die verantwortliche Person zu identifizieren. Wer ist für die Eingabe eines Falls von Kinderpornographie in das Internet verantwortlich? Wer hat bestimmtes

[2] Diese Frage war auch schon Thema eines Grünbuchs und einer Mitteilung der Kommission zum "Grünbuch über Urheberrechte und verwandte Schutzrechte in der Informationsgesellschaft".

urheberrechtliches geschütztes Material abgespeichert? Wer hat die Mehrwertsteuer für die im Online-Bereich angebotene Dienste nicht erklärt?

Angesichts dieses Problems wurde verständlicherweise vorgeschlagen, daß alle, die den Zugriff zum Internet und seinen verschiedenen Online-Diensten suchen, entsprechend identifiziert und alle Online-Tätigkeiten verfolgt werden sollten.

Die Perspektive der Privatsphäre

Die Entwicklung der Politik in bezug auf Internet erfolgt nicht in einem Vakuum, sondern vor dem Hintergrund traditioneller Grundsätze und Werte. Kritiker der Versuche, den Verkehr im Cyberraum einzuschränken oder zu regeln, zitieren das Recht auf freie Meinungsäußerung, ein Grundrecht, das durch Artikel 10 der Europäischen Menschenrechtskonvention gewährleistet wird und als allgemeiner gemeinschaftsrechtlicher Grundsatz in Artikel F.2. des Vertrags über die Europäische Union aufgenommen wurde. Jedoch ist bei der Beurteilung jeglicher auf Internet bezogenen Politik das Recht auf Achtung der Privatsphäre (Artikel 8 EMRK bzw. Gemeinschaftsrecht) genauso wichtig.

In den letzten 25 Jahren hat es sich als eine der größten Bedrohungen des Grundrechts auf die Achtung der Privatsphäre erwiesen, daß Organisationen eine Vielzahl von Informationen über Privatpersonen sammeln können, und zwar in digitaler Form, die sich ihrerseits für eine sehr rasche (und jetzt sehr billige) Handhabung, Veränderung und Mitteilung an andere eignet. Bedenken hinsichtlich dieser Entwicklung und des potentiellen Mißbrauchs dieser personenbezogenen Daten haben alle Mitgliedstaaten (und jetzt mit der Richtlinie 95/46/EG die Gemeinschaft) veranlaßt, besondere Datenschutzgesetze zu verabschieden, die einen Rechtsrahmen für die Verarbeitung personenbezogener Information festlegen.

Ein Grundprinzip des Datenschutzes (siehe Artikel 6 Absatz 1 Buchstabe c und 7 der Richtlinie 95/46/EG) ist, daß die erhobenen personenbezogenen Daten den Zwecken, für die sie bestimmt sind, entsprechen und nicht darüber hinausgehen. Jede persönliche Information ist eine potentielle Bedrohung für die Privatsphäre einer Einzelperson, und es muß daher sichergestellt werden, daß mit dieser Information ein rechtmäßiger Zweck verbunden ist und das Erheben dieser Information auf ein Mindestmaß beschränkt wird.

Ein Merkmal von Telekommunikationsnetzen und Internet insbesondere ist ihr Potential, eine ungeheure Menge transaktioneller Daten (Daten, die generiert werden, um die richtigen Verbindungen sicherzustellen) zu generieren. Durch die Möglichkeiten für eine interaktive Nutzung der Netze (ein Definitionsmerkmal vieler Internet-Dienste) erhöht sich die Menge der transaktionellen Daten noch weiter. Bei Konsultation einer Online-Zeitung interagiert "der Nutzer"durch seine Auswahl der Seiten, die er einsehen möchte. Diese Auswahl erzeugt einen "Clickstream" von transaktionellen Daten. Im Gegensatz dazu werden herkömmlichere Nachrichten und Informationsdienste passiv verbraucht (z.B. Fernsehen), und die Interaktivität ist auf die Offline-Welt von Zeitungsläden und Buchhandlungen begrenzt. Obwohl transaktionelle Daten in einigen der Gerichtsbarkeit unterliegenden Bereichen nach Regeln zum Schutz der Vertraulichkeit des Schriftverkehrs bis zu einem gewissem Grade geschützt sind, gibt die massive Zunahme dieser Daten dennoch Anlaß zu berechtigter Besorgnis.

Mit der zunehmenden technischen Ausgereiftheit und Beliebtheit der Online-Dienste wird das Problem der transaktionellen Daten immer akuter. Überall wo tägliche wir uns in Internet bewegen, hinterlassen wir eine digitale Spur. Da unsere Tätigkeiten im Alltag zunehmend unter Aspekten im Online-Bereich ausgeführt werden, werden auch zunehmend unsere Handlungen, Entscheidungen, Vorlieben aufgezeichnet werden.

Aber die Gefahren für unsere Privatsphäre liegen nicht nur in der Existenz großer Mengen von personenbezogenen Daten im Internet, sondern auch in der Entwicklung von Software, die das Netz suchen und alle verfügbaren Daten über eine genannte Person zusammenstellen können. Ein kürzlich in der *Minneapolis Star Tribune* erschiener Artikel erklärt, wie eine detaillierte Biographie einer aufs Geratewohl ausgewählten Person angefertigt werden konnte, indem derartige Software verwendet und Informationen aus allen Diskussionsgruppen, an denen der Betreffende teilnahm, verwendet wurden. Die Zeitung konnte sich über Anschrift und Telefonnummer, Geburts- und Ausbildungsort, Beruf und gegenwärtigen Arbeitsplatz, Interesse an Amateurtheater, die bevorzugte Biersorte, bevorzugte Restaurants und Ferienziele und Ansichten über verschiedene Themen wie Bill Gates und den sozial repressiven Staat Indiana informieren. An einer Reihe von Orten in den Vereinigten Staaten werden solche "Look-up-Dienste" bereits gewebsmäßig angeboten.

Anonyme Daten - ein Weg, um an die Fragen der Achtung der Privatsphäre heranzugehen

Transaktionelle Daten sind nicht nur eine Bedrohung für die persönliche Privatsphäre, wenn sich die Daten auf eine identifiziere Person beziehen. Eindeutig wäre eine Möglichkeit, auf Bedenken hinsichtlich der Achtung der privaten Sphäre zu reagieren, der Versuch zu gewährleisten, daß - soweit es machbar ist - die durch die Benutzung von Internet geschaffenen Spuren nicht ermöglichen, den Benutzer zu identifizieren. Ist die Anonymität gewährleistet, könnten Einzelpersonen an der Internet-Revolution teilnehmen ohne zu befürchten, daß jede ihrer Bewegungen aufgezeichnet und Informationen über sie abgespeichert werden, die später für Zwecke verwendet werden, die sie ablehnen.

Das Bedürfnis nach Anonymität in Online-Kommunikationen wird in bestimmten Situationen bereits als durchaus berechtigt anerkannt, beispielsweise wenn Opfer einer sexuellen Aggression oder Alkohol- oder Drogensüchtige Erfahrungen mit anderen auszutauschen wünscht, wenn ein einzelner, der sich mit Selbstmordgedanken trägt, spezielle Online-Hilfe in Anspruch nehmen will oder wenn jemand ohne Angst vor Rache über ein Verbrechen aussagen will. In anderen Situationen dient die gewährleistete Anonymität dazu, nicht nur die Achtung der privaten Sphäre, sondern auch die Meinungsfreiheit zu schützen, wie in Fällen, in denen Dissidenten, die Bürger eines totalitären politischen Regimes sind, ihre Opposition gegen das politische System, in dem sie leben, zum Ausdruck bringen und auf Mißbräuche von Menschenrechten aufmerksam machen wollen.

Aber das Bedürfnis nach Anonymität reicht noch sehr viel weiter als in diesen besonderen Fällen. Allein dadurch daß es sie gibt, schaffen identifizierbare transaktionelle Daten ein Mittel, durch das persönliches Verhalten in einem Maße bewacht und kontrolliert werden kann wie nie zuvor.

Abstimmung der privaten Sphäre mit anderen ordnungspolitischen Zielen

Daher steht die Frage der Anonymität im Internet eindeutig im Mittelpunkt eines Dilemmas für Regierungen und internationale Organisationen. Einerseits ist die Möglichkeit, anonym zu bleiben, wesentlich, wenn die Grundrechte auf Achtung der Privatsphäre und freie Meinungsäußerung im Cyberraum bewahrt werden sollen. Andererseits erstickt die Fähigkeit zur Online-Teilnahme und Kommunikation ohne Offenbarung der eigenen Identität schon im Keim die Initiativen, die gegenwärtig für andere ordnungspolitische Kernbereiche entwickelt werden, wie die Bekämpfung illegaler und schädigender Inhalte, Finanzbetrug oder Verstöße gegen das Urheberrecht.

Natürlich ist eine solche offensichtliche Kollision zwischen verschiedenen ordnungspolitischen Zielen nicht neu, und wie das Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten hervorhebt, setzt die Europäische Menschenrechtskonvention bereits einen Rahmen für die Lösung solcher Konflikte: eine Anzahl von Grundrechten vorbehaltlich bestimmter Beschränkungen aus genau bestimmten Gründen, einschließlich der Verbrechensverhütung. Mit Rücksicht auf diese Beschränkungen hat das Fallrecht des Europäischen Gerichtshofes für Menschenrechte, den *Grundsatz der Verhältnismäßigkeit* als der entscheidenden Probe für die Konformität jeglicher zur Anwendung auf die durch die Konvention gewährleisteten Grundrechte bestimmten restriktiven Maßnahme entwickelt.

.

Die Tatsache, daß dieses Fallrecht entwickelt wurde, beweist, daß es seit jeher notwendig gewesen ist, kollidierende ordnungspolitische Zielsetzungen miteinander in Einklang zu bringen. Im Zusammenhang mit den traditionelleren Kommunikationsarten im Offline-Bereich, wie Brief- und Paketpost, Telefon, Zeitungen oder Rundfunk und Fernsehen wurde ein ausgewogenes Verhältnis zwischen diesen Zielen hergestellt Gegenwärtig stehen Entscheidungsträger vor der Herausforderung sicherzustellen, daß dieser ausgewogene Ansatz, der Grundrechte gewährleistet, zugleich aber unter begrenzten und ganz bestimmten Umständen verhältnismäßige Beschränkungen dieser Rechte erlaubt, in dem neuen Cyberraumkontext s beibehalten wird. Im Vordergrund werden dabei das Ausmaß und die Grenzen der Fähigkeit einzelner zur anonymen Online-Teilnahme stehen.

Aus der Vergangenheit lernen, um Lösungen für die Zukunft zu finden

Es besteht ein eindeutiges Einvernehmen darüber, daß die Tätigkeit im Internet nicht von den sonst angewandten Rechtsgrundsätzen ausgenommen werden darf. Internet ist kein gesetzloser Freiraum, in dem die Regeln der Gesellschaft nicht gelten. Gleichermaßen sollte aber die Fähigkeit von Regierungen und Behörden, die Rechte einzelner zu beschränken und potentiell rechtswidriges Verhalten zu überwachen, im Internet nicht größer als in der Offline-Außenwelt sein. Das Erfordernis, daß Beschränkungen der Grundrechte und Grundfreiheiten im Hinblick auf andere Ziele der öffentlichen Ordnung angemessen gerechtfertigt, notwendig und verhältnismäßig sind, muß auch im Cyberraum gelten.

Dieser Grundsatz, Internet nicht besser oder schlechter als ältere Technologien zu behandeln, ist aus der Einleitung der Mitteilung der Kommission über illegale und schädigende Inhalte im Internet, die erklärt "was offline illegal ist, ist auch online illegal" ebenso wie aus dem Bericht der Arbeitsgruppe Illegale und Schädigende Inhalte im Internet ersichtlich, die in ihrem zweiten Vorschlag für ein weiteres Vorgehen den Grundsatz aufstellt, daß für Information im Internet der gleiche freie Informationsfluß wie für papierbezogene Information zulässig sein sollte.

In der Kernfrage der Anonymität sollte dieser Ansatz ebenfalls zugrunde gelegt werden. Wie in der Bonner Ministererklärung[3] zurecht festgestellt wird, sollte grundsätzlich davon ausgegangen werden, daß die Wahl des Nutzers, wenn er die Wahl hat, im Offline-Bereich anonym zu bleiben, diese Wahl auch im Online-Bereich haben sollte. Die über Internet verfügbaren Dienste und Tätigkeiten müssen geprüft und -sofern es möglich ist-, Ähnlichkeiten mit bestehenden Diensten festgestellt werden, die ältere traditionellere Kommunikationsarten und Übertragungsmittel nutzen. Solche Vergleiche gewähren eine nützliche Einsicht in diejenigen Bereiche, in denen die Wahrung der Anonymitiät erstrebenswert wünschenswert ist, und in diejenigen, bei denen dies nicht der Fall ist.

E-mail (Punkt-zu-Punkt-Kommunikation über das Internet)

---

3 Ministererklärung der Ministerkonferenz in Bonn war globale Informationsnetze, 6. bis 8. Juli 1997.

Gegenwärtig identifizieren die meisten E-mail-Mitteilungen den Absender entweder aufgrund seiner eigenen E-mail-Anschrift oder IP-Anschrift. Diese Information ist gewöhnlich für den E-mail-Empfänger genauso wie für die an dem des E-mail-Diensteangebot beteiligten Zugangs- und Diesteanbieter verfügbar, jedoch bieten zwei Arten von Vereinbarungen ein gewisses Maß an Anonymität:

1) anonyme Re-mail-Dienste - wenn der Zugangsanbieter eine Lösung anbietet oder wenn eine Privatperson einen speziellen anonymisierenden Dienst nutzt, an den sie E-mail richtet. Der anonyme Re-mailer versendet die Nachricht in anonymer Form;

2) der anonyme Netzzugang - wenn eine Privatperson anonymen Zugang zu Internet erhält, indem sie beispielsweise im voraus für eine bestimmte Online-Zeit zahlt und eine anonyme E-mail-Anschrift erhält oder den Netzzugang durch einen öffentlichen Internet-Kiosk erhält.

Anonyme Re-mailing-Dienste setzen die Beibehaltung einer Verbindung zwischen dem Absender der Nachricht und der Nachricht selbst voraus, die zu einem späteren Zeitpunkt, beispielsweise im Zusammenhang mit einer polizeilichen Untersuchung rekonstituiert werden kann. Sie gewährleistet daher die Anonymität nicht in der gleichen Weise, wie dies bei der anderen Lösung der Fall ist, und es muß geregelt werden, wie der Re-mailing-Dienst die von ihm aufbewahrten identifizierbaren Daten nutzt. Nichtsdestoweniger haben beide Möglichkeiten bedeutende Vorteile hinsichtlich des Schutzes der Privatsphäre für Privatpersonen und müssen beibehalten und weiterentwickelt werden.

Die Möglichkeit einer anonymen Wahl der E-mail-Lösung ist besonders wichtig, wenn man diesen Dienst mit anderen herkömmlichen und "Punkt-zu-Punkt"-Kommunikationstechnologien vergleicht. So ist beispielsweise der altmodische Postdienst die weitaus privatsphärenfreundlicher, da ein normales Schreiben ganz anonym versandt werden kann. Der Postdiensteanbieter kann keine identifizierbaren transaktionellen Daten über den Absender der Nachricht sammeln (es sei denn, der Absender entscheidet sich für die Anzeige seiner Anschrift auf dem Umschlag). Das weitverbreitetste Zahlungssystem (die Briefmarke) ist also ganz anonym. Der Absender eines Schreibens kann also auch gegenüber dem Empfänger anonym bleiben.

Die herkömmlichen Telefondienste bieten ebenfalls mehr Anonymität als E-mail. Das weitverbreitete Angebot öffentlicher Kioske ermöglicht den anonymen Netzzugang, und Dienste können cash oder mit anonymen Zahlungskartenbeglichen werden. Bei so geführten Telefongesprächen entstehen keine identifizierbaren Servicedaten. Wenn ein Teilnehmer sein eigenes Privattelefon für Anrufe benutzt, entstehen jedoch transaktionelle Daten, und es mußten Datenschutzregeln eingeführt werden (die nach der ISDN-Richtlinie [4] harmonisiert werden), um die Aufbewahrungszeit für diese Daten und die Zwecke, für die sie genutzt werden können, zu begrenzen. Der Anrufende wird indes für den Angerufenen anonym bleiben, bis der Angerufene beschließt den Telefonhörer abzunehmen, wenn nicht die Möglichkeit einer Rufnummernanzeige (CLI) zur Verfügung

---

[4] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 97 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation.

steht, so daß der angerufene Teilnehmer die Möglichkeit hat, eingehende Anrufe vor der Beantwortung abzuhören. Die Auswirkung von CLI auf die Privatsphäre von Teilnehmern an Telefondiensten ist jedoch dergestalt, daß es für notwendig gehalten wurde, durch einen besonderen Artikel in der genannten Richtlinie sicherzustellen, daß Privatpersonen die Anzeige ihrer Rufnummer unterdrücken können. Diese Bestimmung stellt einen Präzedenzfall dar, der bei der "Punkt-zu-Punkt" -Korrespondenz im Online-Bereich berücksichtigt werden kann.

Unter bestimmten Umständen können Beschränkungen der anonymen E-mail-Kommunikation gerechtfertigt sein, beispielsweise wenn Anlaß zu der Vermutung besteht, daß eine besondere Kommunikation mit der Planung einer terroristischen Handlung oder einem sonstigen schwerwiegenden kriminellen Vergehen verbunden ist. Derartige Beschränkungen können bewirken, daß ein anonymer Re-mailer die eigentliche Identität der Teilnehmer einer Kommunikation der Polizei mitteilt, jedoch sollten derartige Beschränkungen den Grundsatz der Datenverhältnismäßigkeit beachten und streng von Fall zu Fall angewandt werden.

Newsgroups, Bulletin Boards und andere öffentliche Diskussionsforen

Die Kommunikation über Internet erfolgt nicht in Form einer "Punkt-zu-Punkt" privaten Korrespondenz. "Newsgroups" und "chat rooms" über besondere Themen oder gemeinsame Interessen sind zahlreich und sehr beliebt. Hier tragen Privatpersonen Material in der Kenntnis bei, daß es für ein breiteres Publikum zugänglich gemacht werden soll, das auch Kinder oder andere schutzbedürftige Privatpersonen umfaßt. In diesem Fall bestehen echte Bedenken hinsichtlich der Art des beizutragenden Inhalts und ein wirkliches Bedürfnis sicherzustellen, das unangemessene Inhalte in solchen offenen Foren kein unangemessener Inhalt angeboten wird und/oder daß eine Haftung besteht, wenn sich ein angebotener Inhalt als illegal erweist.

Es gibt verschiedene Möglichkeiten, um ein gewisses Maß an Kontrolle über derartige "Newsgroups" auszuüben. Ein Vorschlag lautet dahingehend, daß alle Beiträge identifizierbar sein sollten und eine Datenspur erhalten bleibt, wenn Material beigetragen wird. In Frage steht allerdings, ob dies eine verhältnismäßige und wirklich praktikable Antwort auf das Problem gibt. Letztlich gibt es in der nichtvirtuellen Welt zahlreiche Anschlagtafeln am Arbeitsplatz, in der Schule und Hochschule, die Privatpersonen zur Anbringung von Material auffordern. Es ist unvorstellbar, daß der Zugang zu solchen Anschlagtafeln in dieser Weise streng überwacht würde.

Es gibt jedoch noch andere Möglichkeiten. So können Vertragslösungen entwickelt werden, um ein bestimmtes Maß an "inhaltlicher Qualität" zu gewährleisten. Der Anbieter des "Newsgroup"-Dienstes könnte die andauernde Beteiligung eines Moderators in "Newsgroups" sicherstellen der zur Aufgabe hätte, Beiträge auf illegalen und schädlichen Inhalt hin zu überwachen. Diese Moderatoren könnten sicherstellen, daß unangemessene Inhalte rasch entfernt und Personen, die dabei sind dieses Material zu verbreiten, von der Gruppe ausgeschlossen werden. Telefonische "Chat lines" und "Party lines" haben diese Mechanismen seit jeher angewandt, um das Verhalten von Teilnehmern zu mäßigen. Es ist sogar möglich, daß der Dienstanbieter für das zur Verfügung gestellte Material bis zu einem gewissen Grade rechtlich haften muß und so ein unmittelbares Interesse daran hat, alles eingehende Material zu prüfen und nur das zu veröffentlichen, was als rechtmäßig und annehmbar für den öffentlichen Verbrauch gilt. In diesem Szenario kann die

Anonymität von Beitragenden gewahrt werden, während der Dienstanbieter eine ähnlichen Rolle wie der Herausgeber der Leserbriefe einer Zeitung übernimmt.

Auch in diesem Bereich könnten technologische Lösungen eine Rolle spielen. Sollte ein völlig anonymer Zugang zu den gleichen öffentlichen Foren für problematisch gehalten werden, könnten ähnlich wie die vorstehend genannten anonymen Re-mailer einzelne den Zugang aufgrund einer Pseudoidentität, die ihnen ein Fachdienstanbieter verleiht, erlangen. In diesen Fällen könnte eine Verbindung zu der wahren Identität des einzelnen Nutzers rekonstruiert werden, wenn der Verdacht einer kriminellen Tätigkeit besteht, während in der Regel die Anonymität respektiert würde. Natürlich entstehen durch ganz anonyme Beiträge zu öffentlichen Diskussionsforen Schwierigkeiten, die bei der einfachen Punkt-zu-Punkt-Kommunikation nicht auftreten, und müssen geeignete Mechanismen entwickelt werden, um den Mißbrauch solcher Foren zu verhindern. Jedoch dürfen die Grundrechte der Privatsphäre und der Meinungsfreiheit nicht durch Informationspflichtsysteme unangemessen beschränkt werden, besonders wenn es noch angemessenere Mittel gibt, um Inhalte zu überwachen und abzuschwächen.

Passive Suche über Internet WWW

Die meisten heutigen WW-Standorte bestehen hauptsächlich darin, Informationen für die breite Öffentlichkeit anzubieten, und Millionen Menschen verbringen ihre Zeit im Online-Bereich mit der unnützen Suche nach der Unzahl verschiedener angebotener Sites.

Am ehesten ließe sich diese Praxis in der nichtvirtuellen Welt mit der Suche in einer Bibliothek oder einer Buchhandlung oder dem Window-Shopping in der Hauptstraße vergleichen. Wie bei der Online-Suche besteht häufig gar keine Kaufabsicht, sonder es regt sich nur die Neugier um zu sehen, was angeboten wird. Während aber die Suche in einer Buchhandlung oder der Bummel durch die Hauptstraße fast ganz anonym bleiben kann, hinterläßt die Suche über Web eine dauernde und identifizierbarer digitale Aufzeichnung.

Eine ordnungspolitische Begründung oder Begründung im öffentlichen Interesse dafür, daß diese Spuren identifizierbar sein müssen, gibt es nicht, es sei denn der Nutzer wünscht dies. Natürlich sind die Namen und E-mail-Anschriften von Besuchern eines kommerziellen website häufig wertvolle Daten für den website-Inhaber, der möglicherweise die Daten für kommerzielle Zwecke nutzen will. Jedoch muß jede Erhebung derartiger Daten über Privatpersonen, die einfach suchen, völlig transparent sein und mit der Zustimmung des Nutzers erfolgen. Privatpersonen, die anonym über World Wide Web suchen wollen, müssen dazu ungehindert in der Lage sein.

Waren- und Dienstleistungskäufe über Internet

Da sichere Zahlungsmittel entwickelt werden, wird das Internet zusammen mit Mechanismen für Datenintegrität und Beglaubigung von Transaktionen (z.B. digitale Unterschriften) zunehmend zu einem erfolgreichen Geschäftsbereich werden, den Privatpersonen nicht nur zur Information, sondern auch für den Erwerb von Gütern und Leistungen in Anspruch nehmen. In diesem Zusammenhang stellt sich die Frage, ob eine Privatperson, die Einkäufe über Internet tätigen will, identifizierbar sein muß oder anonym bleiben können sollte.

Im nichtvirtuellen Wirtschaftsleben ist die anonyme Barzahlung allgemein üblich, und tatsächlich gilt dies als die bequemste und wirksamste Zahlungsweise für Güter und Leistungen, insbesondere wenn es dabei um verhältnismäßig geringe Geldmengen geht. Der Verkäufer in einem kleinen Eckgeschäft ist nicht an der Identität seines Kunden, sondern nur daran interessiert, daß ihm das Bargeld zum amtlichen Kurs angeboten wird.

Bei größeren Käufen ist es oft für beide, den Käufer und den Verkäufer, lästig, bar zu bezahlen. Banknoten nehmen in der Brieftasche oder in einer Kasse viel Platz ein. Außerdem ist es ein Risiko, soviel Bargeld aufzubewahren. Aus diesen Gründen werden nichtanonyme Zahlungsmethoden wie Schecks oder Kreditkarten, wenn es sich um hohe Beträge handelt, eher vorgezogen.

Natürlich ist die Anonymität bei Kreditkäufen nicht mehr möglich. Bei Kreditkäufen haftet der einzelne für die eingegangene Verbindlichkeit. Daher muß in einer Aufzeichnung die Verbindung zwischen dem Betreffenden und der Verbindlichkeit festgehalten werden. Wenn eine herkömmliche Kreditkarte benützt wird, haftet der einzelne nicht unmittelbar gegenüber dem Verkäufer, sondern gegenüber dem Aussteller der Karte, doch ist eine identifizierbare Spur der Transaktion erforderlich.

Der elektronische Verkehr über das Internet sollte grundsätzlich nach dem Model für Offline-Zahlungen erfolgen. Einzelpersonen sollten zwischen verschiedenen sicheren Zahlungsmethoden wählen können, unter anderem die Möglichkeit eines anonymen Zahlungssystems. Das anonyme electronic cash - System müsste gegenüber der herkömmlichen Barzahlung tatsächlich einige bedeutende Vorteile aufweisen, die ihren Gebrauch sogar noch reizvoller machen würden. Erstens könnten unbegrenzte Beträge, beispielsweise auf einer kleinen Karte aufgenommen werden. Zweitens könnte die Karte ohne daß ihre Anonymität dadurch beeinträchtigt wird, bestimmte Sicherheitsfaktoren die so daß sich das Risiko, wenn die Karte verloren ginge, stark verringern würde. Dadurch könnte das anonyme ec Zahlungssystem bei größeren Online-Käufen attraktiv werden.

Ein Haupterfordernis ist, daß dieses ec "nachweisbar" "wirkliches" Geld ist. Das setzt die Einbeziehung technischer Merkmale der Fälschungsbekämpfung voraus, die die Echtheit des elektronischen Bargeld gewährleisten, ohne die Möglichkeit seiner anonymen Verwendung zu beeinträchtigen.

Jedoch müssen bei der Beurteilung, ob anonym Online-Zahlungsmethoden wünschenswert sind, noch andere ordnungspolitische Erwägungen berücksichtigt werden. Eine Haupterwägung davon ist die Bekämpfung der Geldwäscherei. Die Wäsche der Erlöse aus kriminellen Tätigkeiten wie dem Drogenhandel anonym oder mit einer Scheinidentität ist ein schwerwiegendes Problem. Als Beitrag zur Bekämpfung dieser Tätigkeit wurde 1991 eine Richtlinie (91/308/EWG) zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche verabschiedet. Gemäß den Bestimmungen dieser Richtlinie müssen die Kredit- und Finanzinstitute von ihren Kunden die Bekanntgabe ihrer Identität verlangen, wenn sie zu ihnen in Geschäftsbeziehungen treten, und von den Transaktionen Aufzeichnungen mindestens fünf Jahre lang aufbewahren.

An sich ist diese Richtlinie jedoch nicht unvereinbar mit anonymer Zahlung. Sie betrifft hauptsächlich Transaktionen mit Banken und anderen Finanz- und Kreditinstituten[5], während anonyme ec-Zahlungsysteme wesentlich für Transaktionen zwischen Einzelpersonen und Händlern, die nicht zum Finanzsystem gehören, in Anspruch genommen werden. In der Regel hätte eine Einzelperson ihre Identität nachzuweisen, bevor sie electronic cash von einer Bank entnimmt und vielleicht auch große Mengen electronic cash hinterlegt. Sobald aber dieses cash an seinem Platz ist, gibt es keinen Grund, warum es nicht genauso wie die herkömmlichen Zahlungsmittel anonym sein sollte. Der Bedarf der Polizei und der Rechtsvollzugsinstanzen, die Geldwäschern auf die Spur kommen wollen, muß daher sehr sorgfältig gegen die Vorteile der anonymen Zahlungen für die Privatsphäre aufgewogen werden Es könnte erforderlich werden, daß der Benutzung der anonymen Zahlungsmittel Grenzen gesetzt werden müssen, doch nur dann, wenn eindeutig der Nachweis dafür erbracht ist, daß die Anonymität einer Transaktion tatsächlich die Aufdeckung von Geldwäsche beeinträchtigt. Kleine Transaktionen dürften in dieser Beziehung problemlos sein, und selbst größere Transaktionen (z.B. der Online-Kauf von teurer Software) sind wahrscheinlich keine Geldwäschemittel.

ZUSAMMENFASSUNG DER WICHTIGSTEN SCHLUSSFOLGERUNGEN

- Die Möglichkeit, sich für die Anonymität zu entscheiden, ist wesentlich, wenn Einzelpersonen für ihre Privatspäre im Online-Bereich den gleichen Schutz wie gegenwärtig im Offline-Bereich bewahren sollen.

- Anonymität ist nicht unter allen Umständen zweckmäßig. Die Bestimmungen der Umstände, unter denen die bei der "Anonymität" zweckmäßig ist und der Umstände, unter den dies nicht der Fall ist, erfordert das sorgfältige Abwägen von Grundrechten, nicht nur des Grundrechts auf Achtung der Privatsphäre, sondern auch des Grundrechts auf Meinungsfreiheit, gegenüber anderen wichtigen ordnungspolitischen Zielen, wie der Verbrechensverhütung. Gesetzliche Beschränkungen des Rechts, anonym zu bleiben, oder der technischen Mittel hierfür (z.B. Verfügbarkeit von Verschlüsselungsprodukten), die von Regierungen vorgeschrieben werden, sollten stets angemessen und auf das für den Schutz eines spezifischen öffentlichen Belangs in der demokratischen Gesellschaft notwendige Maß begrenzt sein.

- Soweit dies möglich ist, sollte die Bilanz, die in bezug auf vorhergehende Technologien gezogen wurde, für das Diensteangebot über das Internet beibehalten werden.

- Der E-Mail-Versand, die passive Suche über WWW und der Kauf der meisten Güter und Dienste über das Internet sollten sämtlich anonym ausgeführt werden können.

- Einige Regelungen für Einzelpersonen, die Inhalte zu öffentlichen Foren im Online-Bereich (news-groups usw.) beitragen, sind notwendig, doch die Bedingung, daß

---

[5] Artikel 12 enthält eine Bestimmung, die zum Ergebnis haben kann, daß ihr Anwendungsbereich ausgedehnt wird und Geschäftsbereiche wie Spielkasinos und der Handel mit Wertgegenständen (Kunst, Antiquitäten, Immobilien, Edelmetalle) erfaßt werden können.

Einzelpersonen ihre Identität ausweisen müssen, ist in vielen Fällen unverhältnismäßig und unpraktisch. Andere Lösungen sind vorzuziehen.

- Anonyme Mittel für den Zugang zu Internet (z.B. öffentliche Internet-Kioske, Zahlungskarten) und anonyme Zahlungsmittel sind zwei wesentliche Elemente für eine wirkliche Online-Anonymität.

Umsetzung der Ergebnisse in die Praxis - anwendbare Empfehlungen

In den vorstehenden Schlußfolgerungen, die grundlegend auf das Ausmaß des legitimen Rechts der Einzelperson auf Anonymität im Kontext des Internet eingehen, wird umrissen, welche Verhältnisse geschaffen werden müssen, damit die Privatsphäre von Einzelpersonen nicht untergraben wird. Die gegenwärtige Lage ist eine ganz andere. Der Zugang der Benutzer zum Internet und ihre Tätigkeit sind sehr selten anonym. Bemühungen, halb-anonyme Dienste anzubieten (z.B. anonyme Weiterversendung), haben zu Regelungsproblemen geführt, die technische Gestaltung in Internet-Protokollen läßt keine wirkliche Anonymität zu, und die Kreditkarte bleibt das verbreitetste Zahlungsmittel im Online-Geschäftsverkehr, während Experimente mit anonymen ec-Zahlungsmitteln erst noch in den elektronischen Hautmarkt eindringen müssen.

Damit sich dieses Bild ändert, müssen Wege gefunden werden, um die Schlußfolgerungen in die Praxis umzusetzen. Hierfür sollten Maßnahmen auf verschiedenen Ebenen getroffen werden:

1) Regelungsumfeld

- Der Grundsatz, daß die Sammlung identifizierbarer personenbezogener Daten auf das absolute Minimum begrenzt werden sollte, muß bei der Herausarbeitung nationaler und internationaler Gesetze über Internet anerkannt werden. Ebenso sollte er in Verhaltenskodizes, Leitlinien und anderen “soft law”-Instrumenten, die entwickelt werden, verankert werden. Soweit es sachdienlich ist, sollte dieser Grundsatz auch bestimmen, daß einzelne Benutzer die Wahl haben, anonym zu bleiben.

2) Technologisches Umfeld

- Erörterungen im WWW-Konsortium sollten im Hinblick auf die Entwicklung von Internet - Infrastruktur und Protokollen, die der anonymen Benutzertätigkeit förderlich sind, intensiviert werden.

- Die Mittelausstattung für Forschung und Entwicklung (wie sie im Rahmen des fünften Rahmenprogramms für Forschung und technologische Entwicklung der Gemeinschaft angeboten wird) sollte speziell auf Vorhaben abgestellt sein, mit denen anonyme Zahlungsmittel über das Internet und anonyme Zugriffsmittel (z.B. öffentliche Internet-Terminals) entwickelt werden sollen.

3) Wirtschaftliches Umfeld

- Die Regierungen sollten prüfen, in welcher Weise wirtschaftliche Unterstützung geboten werden kann, um zur weitverbreiteten Einführung von Technologien im Markt anzuregen, stärker schützen und ermöglichen, daß die Einzelperson anonym bleibt.

Beispielsweise könnte eine Regierung ihre Marktmacht als Hauptkunde für IT-Produkte und Dienste nutzen und als Kriterium für ihre eigenen öffentlichen Aufträge Anforderungen hinsichtlich der Privatsphäre und Anonymität stellen. Ebenso könnten Überlegungen über die Förderung privatsphärenfreundlicher Produkte durch Zuschüsse oder Steuervorteile angestellt werden, wie das bei umweltfreundlichen Gütern, etwa bei bleifreiem Benzin der Fall ist.

4) Wachsendes Bewußtsein bei Internet-Benutzern, Zugangs- und Diensteanbietern und in der IT-Industrie

- Den meisten Internet-Benutzern sind die Risiken, die durch ihre Online-Tätigkeit für die Privatsphäre entstehen, nicht bekannt. In dieser Hinsicht besteht ein dringender Beratungs- und Orientierungsbedarf. Den Datenschutzbehörden überall in der Welt fällt bei dieser Beratung eine wichtige Aufgabe zu. Die von der spanischen Datenschutzkommission erarbeiteten Orientierungen zeigen den Weg. Es müssen nunmehr Überlegungen angestellt werden, wie die größtmögliche Verbreitung dieser Beratung für die Internet-Gemeinschaft sichergestellt werden kann.

- Ebenso müssen alle, die Daten über das Internet erheben und verarbeiten (Zugangs-,Diensteanbieter, websites) unterrichtet werden, daß für sie bereits bestehende Datenschutzgesetze gelten, die u.a. die Transparenz und Offenheit bei der Sammlung von Daten vorschreiben und die Zwecke, für die personenbezogene Daten verwendet und offengelegt werden können, beschränken.