9. Digitale Spuren

Beispiel: Tauschbörsen und Abmahnkanzleien

Da Lisi (14) erfahren hat, dass das brandaktuelle Album ihrer Lieblingsband jetzt über eine Internet-Tauschbörse verfügbar ist, schwänzt sie den Ethik-Unterricht, begibt sich stattdessen in ein Kaffeehaus mit kostenlosem Internetzugang, startet auf ihrem Notebook das Programm eMule und lädt das begehrte Album herunter. Zwei Monate später erhält der Kaffeehauspächter, Herr Petersen, einen Brief der Kanzlei „Zocker & Partner Rechtsanwälte OEG", in welchem ihm das Herunterladen urheberrechtlich geschützter Inhalte zur Last gelegt wird. Weiters wird Herr Petersen in dem Schreiben aufgefordert, angefallene Spesen in Höhe von EUR 80,- zu ersetzen, um somit einer Klage zu entgehen. Da Herr Petersen sich keiner Schuld bewusst ist und das Schreiben ignoriert, erhält er im Abstand von jeweils sechs Wochen zwei Mahnungen, in denen zusätzlich zum ursprünglichen Betrag auch noch Mahnspesen in Rechnung gestellt werden. Nachdem Herr Petersen auch das dritte Schreiben ignoriert, endet der Spuk so unvermittelt, wie er begonnen hat.

Die Inhaber der Rechte an dem Musikalbum haben die Anwaltskanzlei Kanzlei „Zocker & Partner Rechtsanwälte OEG" mit der Wahrung ihrer Rechte beauftragt. Die Anwaltskanzlei beteiligt sich selbst an einer Tauschbörse im Internet, um urheberrechtswidrige Downloads (meist Filme und Musik) verfolgen zu können. Dabei wird mit Whois-Abfragen und anderen Internet-Werkzeugen ausgeforscht, wem die auf dem Server protokollierten IP-Adressen der Clients zugeordnet sind. Diese Personen werden abgemahnt und zur Zahlung angeblich angefallener Spesen in Höhe von jeweils EUR 80,- aufgefordert.

Tatsächlich haftet grundsätzlich nicht der Anschlussinhaber (als „Access-Provider" im Sinne des Gesetzes) sondern derjenige, dem das Tauschen urheberrechtlich geschützter Dateien nachgewiesen wird. Ob das alleinige Herunterladen (ohne Hochzuladen) zivil- und/oder strafrechtlich erfolgreich belangt werden kann, ist bislang

noch nicht abschließend geklärt. Allerdings bietet derjenige, der über eine Internet-Tauschbörse Dateien herunterlädt, diese üblicherweise auch anderen Benutzern der Internet-Tauschbörse an. Das Anbieten von urheberrechtlich geschützten Daten ist auf jeden Fall rechtswidrig.

Wer elektronisch kommuniziert, hinterlässt unweigerlich Spuren: die Liste der gewählten Rufnummern im Mobiltelefon, die für Verrechnungszwecke gespeicherten Verkehrsdaten beim Mobilfunkbetreiber, „Cookies" im Webbrowser, Zugriffsprotokolle auf Proxy- und Webservern, das Mailserver-Protokoll beim Internet Service Provider (ISP) usw. Die Speicherung und die Nutzung solcher Daten berühren den Kern der Privatsphäre. Allerdings greifen das im Staatsgrundgesetz verankerte Fernmeldegeheimnis und das im Telekommunikationsgesetz 2003 normierte Kommunikationsgeheimnis nicht in jedem Fall. Die Spuren der elektronischen Kommunikation werden einerseits bei der Verfolgung von Straftaten legal ausgewertet, andererseits werden diese Spuren gerade im globalen Internet, das sich dem Einfluss der österreichischen Rechtsordnung weit gehend entzieht, für kommerzielle und teilweise auch für betrügerische Zwecke genutzt.

9.1 Spuren elektronischer Kommunikation über das Internet

Auf dem eigenen Rechner

Vor allem bei der elektronischen Kommunikation über das Internet sind die hinterlassenen Spuren vielfältig. Beispielsweise wird bei der Verwendung eines Webbrowsers schon auf dem eigenen Rechner eine Vielzahl von Informationen gespeichert (abgerufene Dateien im Browser-Cache, Cookies, Liste der besuchten Websites, eventuell auch eingegebene Formulardaten und Kennwörter). Ein Missbrauch solcher Informationen kann vor allem dann nicht ausgeschlossen werden, wenn andere Personen Zugang zum Rechner haben oder wenn sich Spyware oder ein Trojanisches Pferd (siehe folgende Info-Box) auf dem Rechner eingenistet hat.

Info-Box: Trojanische Pferde

Ein Trojanisches Pferd (meist kurz als „Trojaner“ bezeichnet) ist ein scheinbar nützliches Computerprogramm mit einer Zusatzfunktion, die dem Anwender verborgen bleibt. Häufig besteht die Zusatzfunktion darin, ein Schadprogramm auf dem Rechner zu installieren, das auch dann noch läuft, wenn das Trojanische Pferd deaktiviert oder gelöscht wird. Typische Schadprogramme sind in diesem Zusammenhang

- Keylogger, welche die eingegebenen Tastenfolgen (z.B. Benutzernamen und Passwörter) aufzeichnen,
- Sniffer, welche den über den Netzwerkadapter geleiteten Datenverkehr aufzeichnen,
- Backdoor-Programme, mit deren Hilfe der Rechner ohne Wissen des Anwenders ferngesteuert werden kann und
- Rootkits, welche die Schadprogramme vor dem Anwender verstecken.

Trojanische Pferde treten mitunter auch als Browser-Plugins in Erscheinung, wodurch sie Personal Firewalls auf einfache Weise umgehen können. Andere beruhen auf so genannten Exploits, d.h. auf Computerprogrammen, welche eine Schwäche des Betriebssystems oder eines anderen Computerprogramms nutzen, um auf den angegriffenen Rechnern Administrationsrechte (z.B. für die Installation eines Backdoor-Programms) zu erlangen.

Wirksamen Schutz vor Trojanischen Pferden bietet vor allem der Verzicht auf die Verwendung von Computerprogrammen, deren Herkunft unbekannt oder nicht vertrauenswürdig ist. In eingeschränktem Maß schützt auch eine Kombination der üblichen Sicherheitsmaßnahmen:

- Einsatz einer guten Firewall,
- Einsatz und regelmäßige Aktualisierung eines Antivirenprogramms und eventuell eines Spyware-Detektors sowie eines Rootkit-Detektors,

- regelmäßige (am besten automatische) Aktualisierung des Betriebssystems,
- Deaktivierung automatischer Updates der installierten Software, sofern deren Quelle nicht vertrauenswürdig ist,
- Deaktivierung der Autorun-Funktion für auswechselbare Datenträger.

Wie die empfohlenen Schritte im Detail umgesetzt werden, kann aufgrund der Vielfalt von Programmen, Betriebssystemen etc. hier nicht ausführlich dargestellt werden. Wichtig ist daher, sich beispielsweise durch das Nutzen von Internetsuchen die entsprechenden Anleitungen zu besorgen und auch wirklich umzusetzen.
Solche Maßnahmen schützen jedoch nicht, wenn sich das Trojanische Pferd bereits eingenistet und die Wirkung von Firewall und Antivirenprogramm ausgehebelt hat. Auch vor bislang unbekannten, insbesondere vor individuell programmierten Trojanischen Pferden schützen solche Maßnahmen kaum.

Auf anderen Rechnern

Spuren hinterlässt man auch auf jenen Rechnern, mit denen man kommuniziert: Ein Webserver speichert beispielsweise für jede einlangende Anfrage den Namen bzw. die IP-Adresse des anfragenden Rechners, den Zeitpunkt der Anfrage, die Anfrage selbst, einen Statuscode, die Anzahl der übertragenen Bytes und eventuell weitere benutzerspezifische Informationen. Diese Informationen werden nicht nur auf Webservern gesammelt, sondern auch bei der Zwischenspeicherung der abgerufenen Dateien auf so genannten „Proxy-Servern“, welche von zahlreichen ISPs zur Optimierung des Datendurchsatzes verwendet werden. Ein ISP könnte sich daher mit Hilfe der Protokolldateien auf seinen Proxy-Servern über das Surfverhalten seiner Kunden informieren. Die Speicherung solcher Informationen ist jedoch in Österreich in der Regel derzeit unzulässig.

Ähnliche Protokollierungsmechanismen existieren für zahlreiche andere im Internet gebräuchliche Protokolle, z.B. Mail und Usenet (eine Art virtuelles Schwarzes Brett im Internet). Hingegen sind Internet-

Tauschbörsen meistens als dezentrale „Peer to Peer-Netzwerke“ angelegt. Bei diesen agiert jeder an der Tauschbörse beteiligte Rechner zugleich als „Client“ und als Server. Das bedeutet: Jeder Nutzer der Tauschbörse kann auf freigegebene Daten, die auf den Rechnern der anderen Tauschbörsennutzer liegen, zugreifen. Ebenso kann man aber auch auf die Inhalte der anderen Rechner im Tauschbörsenverbund zugreifen und sie herunterladen. Typische Beispiele sind eDonkey2000, Gnutella, BitTorrent, FastTrack etc. Die Datenübertragung wird dabei allenfalls dezentral protokolliert und kann von Außenstehenden weniger leicht nachvollzogen werden als bei traditionellen Download-Verfahren. Die Anonymität wird aber beeinträchtigt, indem die Tauschbörsen-Software auf jedem Rechner über die für das Herunterladen bestimmten Dateien informiert wird und diese Informationen mitprotokolliert. So lassen sich jene Server ausforschen, auf denen Inhalte rechtswidrig bereitgestellt werden. Ein höheres Maß an Anonymität bieten aktuelle Peer to Peer-Netzwerke der Dritten Generation, welche die Identitäten des Senders und des Empfängers durch indirekte Datenübertragung verschleiern und welche den Datenverkehr verschlüsseln (z.B. Waste, ANts, Mute, I2P).

Ein ISP kann in der Regel nachvollziehen, welchem Kunden eine bestimmte IP-Adresse zugeordnet ist. Der Kunde ist aber mit dem Anwender nicht notwendigerweise identisch. Weitgehende Anonymität genießen Anwender in Internetcafés, die neben dem Internetzugang auch Rechner zur Verfügung stellen: die Beziehung zwischen Anwendern und IP-Adressen ist dort kaum nachvollziehbar. Flughäfen, gastronomische Betriebe usw. stellen hingegen häufig Funknetzwerke öffentlich bereit, auf welche die Anwender mit ihren eigenen Rechnern kostenlos zugreifen. In diesem Fall wird bei der Zuweisung einer IP-Adresse meistens auch die MAC-Adresse (das ist eine eindeutige Gerätekennung) des Rechners protokolliert. Da die MAC-Adresse jedoch manipuliert werden kann, ist der Beweiswert der Protokollierung gering. Somit ist die Anonymität auch in kostenlos zugänglichen Funknetzwerken weit gehend gegeben. Anders verhält es sich mit Funknetzwerken kommerzieller Betreiber, bei welchen der Anwender identifiziert wird oder zumindest zu Verrechnungszwecken personenbezogene Daten eingeben muss. Die gegebenenfalls auch zeitabhängige Zuordnung der IP-Adresse zu einem Anwender kann dabei häufig nachvollzogen werden.

9.2 Cookies & Co.

Im Web kann man vollkommen anonym surfen und Webseiten abrufen. Oder doch nicht? Jeder Rechner im Internet kann durch seine IP-Adresse identifiziert werden. Die Zuordnung der IP-Adresse zum Teilnehmer ist entweder fix (statische Adresse) oder dynamisch. Im letzteren Fall erhält der Teilnehmer beim Verbindungsaufbau die nächste freie Adresse aus einem Pool zugeteilt, dabei ist die Zuordnung nur dem Internet Service Provider (ISP) bekannt. Teilen sich mehrere Teilnehmer – etwa in einer Wohngemeinschaft oder in einer Firma – einen gemeinsamen Internetzugang, so kann durch die IP-Adresse nicht mehr genau erkannt werden, von welchem PC aus die Webseite abgerufen wurde. Allerdings kann der PC nicht nur aufgrund seiner IP-Adresse identifiziert werden. Browser speichern beim Abruf einer Seite Daten und übermitteln diese Daten auch bei Abfrage wieder zurück. Es gibt mehrere Verfahren, um derartige Daten zu speichern, die bekannteste Variante sind so genannte Cookies. Damit ist es möglich, Besucher einer Webseite wiederzuerkennen. Bei einem Cookie wird vom jeweilig aufgerufenen Webserver eine Information am jeweiligen Computer abgespeichert. Welche Cookies sich bereits auf dem Rechner befinden, kann man im verwendeten Webbrowser, meist in der Rubrik „Extras“ ablesen. Eine einfache Nutzung von Cookies sind so genannte Session-IDs. Das sind Kennungen, mit denen es dem Webseitenbetreiber möglich ist, aufeinanderfolgende Aufrufe von Seiten zu einer Session eines Users zusammenzufügen. Ein Beispiel eines derartigen Session-Cookies ist in der Abbildung 24 dargestellt.

Die Information sagt aus, dass vom Rechner „webpresentment.uni2.se“ ein Cookie mit dem Namen „PHPSESSID“ übermittelt wurde. Der Inhalt des Cookies ist „d058b...“, eine Zahl, welche am Server mit der aktuellen Session in Beziehung steht. Das Cookie wird am Ende der Session ungültig (verworfen).

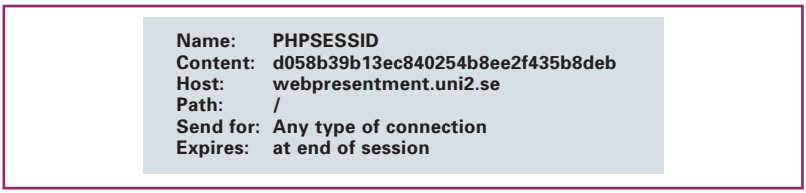

Abbildung 24: Beispiel eines Cookies für eine Session-ID

Nun ermöglichen derartige Cookies lediglich festzustellen, welche Seiten wie lange und in welcher Reihenfolge abgerufen wurden, erlauben jedoch keine Zuordnung zu einer bestimmten Person. Trotzdem kann der Webseitenbetreiber zusätzliche Informationen über Surfverhalten etc. gewinnen. Häufig werden Cookies auch von Webshops verwendet, da sie mit Hilfe von Cookies einen Benutzer wiedererkennen können.

Werden diese Informationen von mehreren Webseiten geteilt, so ist es auch möglich, unter Zuhilfenahme einer Seite, welche z.B. mit Kreditkarteninformationen verknüpft ist, auf konkrete Personen zu schließen: Man surft auf die Website A. Bei dieser wird ein Cookie mit der Information hinterlegt, dass man sich auf der Website A befunden hat. Surft man nun über verschiedene Webseiten zur Website X, kann dieser Betreiber das Cookie auslesen und feststellen, dass sich der Surfer auf der Website A befunden hat. In weiterer Folge könnte der Betreiber der Website X mit den Informationen zur Website A einen Datenabgleich durchführen. Hat der Nutzer beispielsweise auf der Website A ein Produkt gekauft und mit der Kreditkarte bezahlt, so könnte auch der Website-Betreiber der Website X ohne weiteres Zutun die Identität des Nutzers feststellen. Das setzt natürlich einen Informationsaustausch der beiden Website-Betreiber voraus.

Google bietet etwa unter „Google-Analytics“ Webmastern die Möglichkeit, die Nutzung von Webseiten zu analysieren. Ein Betreiber einer Website kann diesen kostenfreien Dienst auf seinem Webserver implementieren. Damit wird es dem von Google betriebenen Server von Google-Analytics möglich, das Nutzungsverhalten der Webseite mitzuverfolgen und dem Betreiber der Webseite Informationen über die Nutzung der Seite zu übermitteln. Da jedoch die Analyse zentral bei Google erfolgt, ergibt sich dadurch grundsätzlich die Möglichkeit, das

Nutzungsprofil von Internetnutzern auf ihrem Weg durch's Internet zu erstellen. Verwendet ein Nutzer auch einen Google-Dienst mit Anmeldung, ist es prinzipiell auch möglich, dieses Nutzungsprofil einer bestimmten Person zuzuordnen.

Alle diese Funktionen und Dienste sind durchaus nützlich, ist es doch praktisch, eine am Vortag besuchte Seite einfach wiederfinden zu können. Doch letztlich erlauben solche Dienste einen tiefen Einblick in die Privatsphäre des Internetnutzers. Insbesondere Google hat in der Vergangenheit immer wieder Wert darauf gelegt, unter dem Motto „Don't be evil" zu handeln. Der Nutzer erhält viele nützliche, meist kostenlose Dienste, welche die Nutzung des Internets erleichtern. Allerdings hinterlässt der Nutzer im Gegenzug eine Vielzahl von Informationen bei Google.

Man muss aber nicht unbedingt aktiv im Internet surfen, um dort seine Spuren zu hinterlassen. Es genügt, ein Programm auf seinem PC installiert zu haben, welches automatisch überprüft, ob Updates – also neuere Versionen von Programmen – verfügbar sind. Der Anbieter der Software erfährt so, auf wie vielen Rechnern ein bestimmtes Programm installiert ist und wie intensiv es genutzt wird – ohne dass zusätzliche Informationen bei der Überprüfung auf Updates, übermittelt wurden.

Info-Box: Wie kann man verhindern, ungewollt Informationen im Internet zu hinterlassen?

Grundsätzlich sollte man persönliche Daten nur dort eingeben, wo die Eingabe für die Leistung tatsächlich notwendig ist und der Datenumfang in einem sinnvollen Verhältnis zur erbrachten Leistung steht. In einem Webshop also etwa Name, Zahlungsinformationen und Adresse.

Gleichzeitig sollte man abwägen, ob der Komfortgewinn einer gegebenenfalls auch kostenlosen Anwendung in einem sinnvollen Verhältnis zum möglichen Verlust an Privatsphäre steht.

Bei vielen Webbrowsern ist es möglich, die Nutzung von Cookies einzuschränken. Es kann etwa der Browser so konfiguriert werden, dass Cookies beim Schließen des Browsers gelöscht werden.

9.3 Vorratsdatenspeicherung

Die Europäische Union (EU) hat sich im Zuge der Terroranschläge von London und Madrid im Jahre 2005 entschlossen, die Möglichkeiten zur Ausforschung von Tätern zu verbessern. Wissenschaftliche Untersuchungen und praktische Erfahrungen in einigen Mitgliedstaaten hätten gezeigt, dass Verkehrs- und Standortdaten für die Ermittlung, Feststellung und Verfolgung von Straftaten von großer Bedeutung sind.

Da immer mehr Kommunikation über den elektronischen Weg wie Mobiltelefon oder Voice over IP (VoIP) geführt wird, sind die Daten über diese Nutzung – laut Europäischer Union – besonders wichtig zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten. Die Daten werden als notwendiges wirksames Ermittlungswerkzeug für die Strafverfolgung gesehen, insbesondere in schweren Fällen wie organisierte Kriminalität und Terrorismus. Die Europäische Union sah sich nun veranlasst, hier gewisse Grundsätze im Rahmen einer Richtlinie vorzugeben.

Diese Richtlinie muss von den Mitgliedstaaten noch ins innerstaatliche Recht umgesetzt werden. Die Umsetzung der Bestimmungen für die Speicherung von Daten betreffend Internetzugang, Internettelefonie und Internet-E-Mail können von den einzelnen Staaten bis 15.03.2009 aufgeschoben werden. Dafür hat sich auch der österreichische Gesetzgeber entschieden. Hinsichtlich Telefonie ist in Österreich allerdings eine zeitnahe Umsetzung noch im Jahr 2007 vorgesehen. Zum Zeitpunkt der Endredaktion wurde die Richtlinie betreffend Telefonie noch nicht in österreichisches Recht umgesetzt.

Von der Vorratsdatenspeicherung sind Verkehrsdaten und Standortdaten umfasst, die zur Feststellung des Teilnehmers oder des Benutzers erforderlich sind. Momentan dürfen in Österreich nur jene Daten gespeichert werden, die für die Verrechnung an den Kunden relevant sind. Dazu gehören z.B. Datum, Uhrzeit, Dauer und Rufnummer eines Telefonats.

Die Richtlinie sieht vor, dass mehr Informationen als bisher über Anrufer, Angerufenen, Internetnutzer etc. gespeichert werden sollen und dass diese im Bedarfsfall an Behörden weitergeleitet werden. Als zu speichernde Daten sind unter anderem die Rufnummer, Name und Anschrift des Anrufers, Benutzerkennung bei Internetzugängen angeführt, aber auch Datum und Uhrzeit bei An-/Abmeldung beim Internetzugang und die IP-Adresse. Weiters sollen Daten über die Art der Nachrichtenübermittlung und der verwendeten Endeinrichtung (IMSI – Kennung des Mobiltelefonkunden, IMEI – Kennung des Mobiltelefons) vom Anrufer und vom Angerufenen und die Daten über den Standort bei Beginn der Verbindung gespeichert werden. Anrufe, bei denen keine Verbindung zustande kommt, sind von der Speicherpflicht nicht umfasst. Von der Speicherung ist der Inhalt der Kommunikation (Sprachinformation oder Texte, SMS oder E-Mails bzw. besuchte Websites) – wie auch bisher – nicht betroffen.

Ein besonders kritischer Punkt der Richtlinie ist die Frage, wer unter welchen Voraussetzungen Zugriff auf die gespeicherten Daten bekommt. Hier wird die Frage heftig diskutiert, bei der Aufklärung welcher Delikte und dem damit verbundenen Strafrahmen ein Zugriff der Strafverfolgungsbehörden auf diese Daten gegeben sein muss. So ist völlig unstrittig, dass bei der Aufklärung eines Mordkomplotts der Zugriff auf Vorratsdaten gerechtfertigt ist. Bei Delikten wie Stalking erscheint es allerdings zweifelhaft, ob der verhältnismäßig schwere Eingriff in die Privatrechte möglich sein muss. Hier wird die entsprechende Entscheidung und Wertung des Gesetzgebers abzuwarten sein.

Die Richtlinie sieht für die Dauer der Datenspeicherung einen Rahmen von mindestens sechs Monaten und höchstens zwei Jahren vor. Die Gesetzgeber der einzelnen Mitgliedstaaten entscheiden, wie lange in ihrem Land die Daten gespeichert werden dürfen. Welchen Rahmen Österreich wählen wird, ist noch nicht entschieden. Wahrscheinlich wird sich Österreich aber für die Minimalfrist von sechs Monaten entscheiden.

Um die Speicherung bzw. die Verwendung der Daten zu kontrollieren, sieht die Richtlinie eine Kontrollstelle vor. Soweit bisher bekannt, wird diese in Österreich bei der Datenschutzkommission angesiedelt werden (Stand Oktober 2007).

Die Vorratsdatenspeicherung stellt einen Eingriff in das Recht auf Achtung des Privatlebens dar. Dieses Recht unterliegt einem besonderen Schutz durch die Grundrechte und da wieder der Europäischen Menschenrechtskonvention (EMRK). Gemäß Artikel 8 EMRK darf in dieses Recht nur dann eingegriffen werden, wenn der Eingriff gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft zur Aufrechterhaltung der Ordnung, zur Verhinderung von Strafdaten etc. notwendig ist. Laut Europäischer Union ist die Vorratsdatenspeicherung ein notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus. Die durch die Vorratsdatenspeicherung erfassten Daten sollen den Strafverfolgungsbehörden für einen bestimmten Zeitraum unter den in der Richtlinie festgelegten Bedingungen zur Verfügung stehen. Dass diese Wertungen nicht völlig unumstritten sind, zeigt sich daran, dass die Planung und Erlassung der gegenständlichen Richtlinie eine europaweite Diskussion und verschiedenste nationale Bewegungen gegen die Richtlinie ausgelöst haben.