ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT 5

(Seiten 301–376) 1999

Datenschutz-RL und DatenschutzG 2000

Finanzierung im Konzern
Reichweite des Ausschüttungsverbots

Dumping durch Hochlohnländer
Ausländische Bauleistungen in der BRD

Umsatzsteuer
Anwaltskostenersatz

Ertragssteuern
Steuerliche Einlagenrückzahlung im Konzern

Memoire der EU-Kommission
Vergabe von Konzessionen

AVG-Novelle 1998
Schluß des Ermittlungsverfahrens

150 JAHRE MANZ

Ernst O. Brandl / Viktor Mayer-Schönberger

CPU-IDS, COOKIES UND INTERNET-DATENSCHUTZ

Transaktionsgenerierte Identifikationsmerkmale werden im Internet immer häufiger gebraucht, um die Anonymität des Netzes zu durchbrechen und persönliche Informationen über den Benutzer zu erhalten. Da dies für den User grundsätzlich unbemerkt geschieht, ergeben sich daraus erhebliche datenschutzrechtliche Bedenken.

Der weltgrößte Hersteller von Computer-Prozessoren, die Firma Intel, ist vor einigen Monaten in die Schlagzeilen geraten, weil bekannt wurde, daß sie ihre Chips mit Seriennummern (sog CPU-IDs) ausstatten wollte, die elektronisch auch über das Internet abgefragt werden können. Nach weltweiten Protesten und Boykottdrohungen von Datenschützern und Anwendern war Intel gezwungen, diesen Plan aufzugeben.

Doch Intels CPU-IDs sind nicht der erste Versuch, im Internet Identifikationsmerkmale zu schaffen. Informationselemente am WorldWideWeb (WWW) – „Cookies" genannt – nehmen bereits seit Jahren weitgehend unbeachtet von den Anwendern eine ähnliche Rolle ein. Diese „Cookies" sind Informationsstücke, die ein Informationsanbieter im WWW erstellt hat und die im Computer des surfenden Anwenders gespeichert werden, bereit für spätere Zugriffe durch den Informationsanbieter. Cookies sind dabei eingebettet in die Informationen, die zwischen Anwender und Informationsanbieter ausgetauscht werden. Die rechtlichen Rahmenbedingungen für den Umgang mit diesen Identifikationsmerkmalen sollen im folgenden kurz dargestellt werden.

1. Der Zweck von Identifikationsmerkmalen im Internet

Wozu braucht man Identifikationsmerkmale, wie CPU-IDs oder Cookies, überhaupt? Ihre Befürworter führen ins Treffen, daß im Internet niemand mit Sicherheit wisse, wer der Kommunikations- und damit auch mögliche Vertragspartner sei. Diese Unsicherheit in der Identifizierung des Gegenübers am Netz lasse viele Anwender zu Recht vor Vertragsabschlüssen im Internet zurückschrecken. Wie kann man die Vertragstreue des anderen richtig einschätzen, wenn man nicht einmal sicher weiß, wer der andere überhaupt ist? Auf das Fehlen der Sicherheit beim Vertragsabschluß wiederum folgt konsequenterweise ein vermindertes Vertrauen der Anwender in das Internet als Medium des elektronischen Geschäftsverkehrs. Will man daher den elektronischen Geschäftsverkehr in Gang bringen – Stichwort „e-commerce" – müsse man technische Maßnahmen einführen, die eine sichere Identifikation der Verhandlungs- und Vertragspartner am Netz erlauben. Genau diese Rolle könnten CPU-IDs, Cookies udgl übernehmen, indem sie den Vertragspartner entsprechend identifizieren.

Wer so argumentiert, hat freilich weder das Internet verstanden noch die Technik dieser Identifikationsmerkmale. Denn CPU-IDs und Cookies beziehen sich auf einen Computer, nicht jedoch zwangsläufig auf eine einzelne Person. Das wäre so, als würde man behaupten, die Telefonnummer alleine sei schon ein hinreichendes Kriterium, die Identität des Vertragspartners festzustellen. In der Wirklichkeit werden jedoch Vertragspartner selten durch Telefonnummern identifiziert, können und werden doch Telefone wie Computer durchaus nicht nur von einer einzigen Person benutzt. Es wäre wohl absurd, alle Handlungen von Personen eines Münztelefons in einem Lokal dem Gastwirt zuzurechnen, nur weil das Telefon auf dessen Namen zugelassen ist. Hinzu kommt, daß das Internet ein offenes Netz ist und jeder ohne große Schwierigkeiten einfach das Identifikationsmerkmal eines anderen vortäuschen kann. Wenn aber jeder, der dies will, ein beliebiges Identifikationsmerkmal angeben kann, dann verliert dieses Merkmal seinen praktischen Nutzen – die Partner können nicht mehr darauf vertrauen.

In der Tat bedarf es weitaus komplexerer technisch-organisatorischer Maßnahmen, um die Identifikation des anderen und die Authentizität seiner Nachrichten sicherstellen zu können. Dazu dient die in letzter Zeit ebenfalls vielzitierte „digitale" oder nach neuerem Jargon nunmehr „elektronische"[1]) Signatur.[2])

2. Transaktions-generierte Informationen (TGI)[3])

Es muß daher wohl einen anderen Grund geben, warum derartige technische Identifikationsmerk-

1) So der nunmehrige Oberbegriff des Entwurfs einer EU-RL; vgl dazu Draft for a European Parliament and Council Directive on a common framework for electronic signatures, Doc 6229/99 EN.

2) Zu Fragen der digitalen Signatur vgl schon *Brenn,* Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ 1997, 641; *Mayer-Schönberger,* Das Recht am Info-Highway (1997) 143ff; *Mayer-Schönberger/Pilz/Reiser/Schmölzer*, Sicher und Echt: Der Entwurf eines Signaturgesetzes, MR 1998, 107; *Mayer-Schönberger*, Österreich und der Geschäftsverkehr im Internet: eine vertane Chance, Homepages 2/98, 21; *Mayer-Schönberger/Pilz/Reiser/Schmölzer,* The Austrian Draft Digital Signatures Act, CLSR 1998, 317; *Mayer-Schönberger/Pilz,* Das Recht am Netz, in Zechner/Doppel/Holzinger (Hrsg), Handbuch Internet (1998) 140 hier 146ff; *Pilz/Mayer-Schönberger,* E-Commerce: Rechtliche Rahmenbedingungen und Notwendigkeiten, AnwBl (in Druck).

3) Der Begriff wurde geprägt von *McManus,* Telephone transaction-generated information: Rights and Restrictions (1990); vgl auch *Schaar,* Datenschutzfreier Raum Internet? CR 1996, 170 hier 172; *Mayer-Schönberger,* Das Recht am Info-Highway (1997) 168ff.

male immer stärkere Verwendung im Internet finden. Der Schlüssel zum Verständnis liegt in der Natur des Internets als digitales Informationsnetz: Kauft man im wirklichen Leben beim Zeitungshändler an der Ecke eine Zeitung, bezahlt in bar, nimmt die Ware Zeitung und geht, verbleiben über diese Transaktion keinerlei Informationen bei Verkäufer und Käufer – keine Quittung, keine Rechnung, keine Überweisung. Im Internet ist dies anders: Jede Transaktion im Internet erzeugt Information – Transaktionssender, Transaktionsempfänger, Transaktionszeit und -datum etc. Diese Information ist in digitaler Form vorhanden und kann – muß aber nicht – technisch nach Ende der Transaktion gelöscht werden. Unternehmen haben nun entdeckt, daß diese transaktionsgenerierten Informationen (TGI) sehr wertvoll sein können: Sie geben Auskunft darüber, welche Waren der Benützer gekauft, welche Informationsangebote im Internet er angesehen, oder auf welche Werbeanzeigen auf Internetseiten er aus Interesse geklickt hat. Je mehr dieser TGI über eine einzelne Person bekannt sind, desto genauer kann ein Bild dieser Person mit ihren Vorlieben und Wünschen, ihren Schwachstellen und Lastern entstehen und auch kommerziell genutzt werden. Interessiert sich jemand für die Informationsangebote von Autoherstellern, plant er vielleicht einen Autokauf und ein versierter Autohändler könnte diese Information verwenden, um dem Betroffenen einschlägige Werbe-E-mails zu senden. Das mag man noch als lästiges Problem unserer Zeit abtun. Informationen hingegen darüber, daß sich jemand am Internet über die Ansteckungsmöglichkeiten von Aids oder auch für eine religiöse Sekte interessierte, könnten – in falsche Hände geraten – durchaus existenzielle Folgen haben.

Die Problematik von TGI ist daher paradoxerweise ihre Omnipräsenz und gleichzeitige Intransparenz: Denn TGI entstehen durch die digitalen Netze bei jeder Transaktion und können dank des digitalen Codes einfach verarbeitet, gespeichert und weitergegeben werden. Den Anwendern hingegen ist diese Tatsache nicht bewußt. Sie sind aus dem täglichen Leben TGI nicht gewohnt und auch im Internet „merkt" man als Anwender das Entstehen und die Weitergabe der TGI nicht. Diese Problematik wird bei sog „Cookies" besonders deutlich:

3. Die Cookies[4])

Cookies gibt es, um Suchmaschinen zu personalisieren,[5]) oder um sicherzustellen, daß ein interessierter Kunde nur einmal an einem Web-Gewinnspiel teilnehmen kann, oder um eine Liste von Waren, die ein Konsument beim Gang durch virtuelle Geschäfte in den Warenkorb gegeben hat, zwischenzuspeichern.[6]) In den meisten Fällen erfolgt nicht nur das Speichern des Cookies am Computer, ohne daß es der Konsument bemerkt, sondern auch die späteren „Zugriffe" der Web-Anbieter auf diese Information. Denn Web-Anbieter erhalten automatisch Zugriff auf alle entsprechenden Cookies, wenn der Konsument mit ihnen in Verbindung tritt, in der Regel, indem er Web-Information aufruft.

4. Der rechtliche Rahmen

Der Schutz persönlicher Daten ist seit Beginn der siebziger Jahre in Europa in nationale Gesetze gefaßt.[7]) Zur Harmonisierung dieses Schutzes auf möglichst hohem Niveau hat die EU 1995 eine RL zum Datenschutz verabschiedet.[8]) Sie wäre im wesentlichen bis 1998 umzusetzen gewesen.[9]) In Österreich ist mit der Verabschiedung des der Umsetzung dienenden Datenschutzgesetzes 2000 (DSG2000) in Kürze zu rechnen. Schon aufgrund dieser Tatsache, aber auch des internationalen Aspekts des Internets bietet sich an, die Cookies im Hinblick auf die EU-RL zum Datenschutz zu untersuchen.

Die RL legt die Bedingungen fest, die für die automatisierte Verarbeitung persönlicher Daten vorliegen müssen. Zu diesen Bedingungen gehört, daß persönliche Daten „auf rechtmäßige Weise" verarbeitet werden müssen und nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden dürfen.[10]) Die Verarbeitung muß „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden". Die Daten müssen dabei „sachlich richtig verwendet und, wenn nötig, auf den neuesten Stand gebracht werden." Sie dürfen nicht länger als zweckentsprechend gespeichert bleiben.[11])

Darüber hinaus dürfen sie nur verarbeitet werden, wenn der Betroffene „ohne jeden Zweifel" seine Einwilligung gegeben hat, oder wenn die Verarbeitung aufgrund einer gesetzlichen oder vertraglichen Verpflichtung gegenüber dem Betroffenen notwendig ist. Ausnahmen erlauben die Verarbeitung im öffentlichen oder vitalen Interesse des Betroffenen, oder wenn keine grundsätzlichen Datenschutzinteressen

4) Vgl dazu *Mayer-Schönberger,* The Internet and Privacy Legislation: Cookies for a Treat? 1 West Virginia Journal of Law & Technology (1997), http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.html; *Mayer-Schönberger,* Cyberlinks: Datenschutz für die Keks? Juridikum 2/97, 39; *Mayer-Schönberger,* Improving Computer Security on the Internet through Novel Legal Venues – Cookies for a Treat? Proceedings eicar '96 (European Institute for Computer Anti-Virus Research) (1996) 155; *Mayer-Schönberger,* Internet Privacy: The Internet and Privacy Legislation: Cookies for a Treat? Computer Law & Securities Report Vol 14 no.3 1998, 166. Der ursprüngliche Cookie-Standard ist erhältlich unter *Netscape,* Persistent Client State HTTP Cookies, Preliminary Specifications, http://home.netscape.com/newsref/std/cookie_spec.html. Der aktuelle Cookie-Standard ist *Kristol/Montulli,* HTTP State Management Mechanism, HTTP Working Group, INTERNET DRAFT, http://portal.research.bell-labs.com/~dmk/cookie.txt, vgl auch die EPIC Cookies Page, http://www.epic.org/privacy/internet/cookies; sowie www.cookiecentral.com; zu den technischen Grundlagen vgl *St.Laurent,* Cookies (1998).

5) Vgl nur MyYahoo! http://my.yahoo.com oder Microsoft's Persönliche Homepage unter http://www.msn.com.

6) Weitere Beispiele und Erläuterungen bieten *St.Laurent,* Cookies (1998).

7) Vorreiter war das 1973 verabschiedete schwedische Datalag (1973:289); eine deutsche Übersetzung findet sich in *Simitis et al,* Data Protection in the European Community – The statutory Provisions (1996). In Deutschland war das Land Hessen führend: Hessisches Datenschutzgesetz vom 7. 10. 1970, GVBl 1970 I, 625; Österreich folgte 1978 mit dem Datenschutzgesetz (DSG), BGBl 1978/565.

8) RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl Nr L 281 vom 23. 11. 1995, 31.

9) Vgl Art 32 RL.

10) Vgl Art 6 RL.

11) Id.

des Betroffenen von der Verarbeitung berührt sind.[12]) Besondere Schutzbestimmungen regeln die Verarbeitung „sensitiver" Daten.[13]) Der Betroffene hat umfassende Rechte auf Auskunft über die über ihn gespeicherten Daten, über den Namen des Verarbeiters, den Zweck der Erhebung und die Namen aller Empfänger der Daten.[14])

5. Datenschutz und Cookies

Eine datenschutzrechtliche Problematik kann freilich nur dann entstehen, wenn Cookies personenbezogene Daten enthalten, an denen ein Geheimhaltungsinteresse des Betroffenen besteht. Cookies können grundsätzlich beliebige Informationen enthalten. Da sie jedoch primär zur Personalisierung der Informationsangebote im Internet dienen, sind sie in aller Regel ein individualisierendes Identifikationsmerkmal, das den Informationsanbieter – sobald er das Cookie erhält – die Wünsche und Präferenzen des Informationssuchenden erkennen läßt. Schon deshalb wird man bei in einem Cookie gespeicherten Daten idR von personenbezogenen Daten sprechen können. Die Frage nach dem Bestehen eines Geheimhaltungsinteresses des Betroffenen wird hingegen vom Einzelfall abhängen.

Klar ist aber, daß aufgrund ihrer Struktur Cookies grundsätzlich gegen die in der RL zum Ausdruck gebrachten Datenschutznormen auf eine ganze Reihe von Arten verstoßen können.

Nach den noblen Zielen des ursprünglichen Standards sollten Cookies zwar bloß für die Dauer der aktuellen Abfrage gespeichert[15]) und bei Beendigung des Surfens automatisch gelöscht werden. Nach den Standardvorgaben kann auf Cookies auch nur von dem Informationsanbieter und der Web-Seite zugegriffen werden, die das Cookie ursprünglich erstellt hatte. Damit sollte die Genauigkeit und Vergänglichkeit der persönliche Daten beinhaltenden Cookies garantiert werden. Leider können aber diese Standardvorgaben überschrieben werden. Ein Informationsanbieter kann die Lebensdauer der Cookies auf mehrere Jahre ausdehnen und festlegen, daß auch andere Web-Seiten auf dem gleichen Server des gleichen Informationsanbieters, ja sogar eine große Zahl von Servern anderer Informationsanbieter auf das Cookie Zugriff bekommen. In der Praxis verwenden sehr viele Anbieter, etwa auch Microsoft, diese Möglichkeit extensiv.

Ganz offensichtlich erlauben daher diese „Optionen" das Umgehen der grundlegenden Datenschutz- und Datensicherheitsprinzipien: Aufgrund ihrer langen „Lebensdauer", können Cookies etwa die Prinzipien der „Richtigkeit" und „Aktualität" von Art 6 der RL verletzen. Darüber hinaus ist sich der durchschnittliche, im Web surfende Anwender des „Cookie-Verkehrs" gar nicht bewußt. Dies verstößt gegen die umfassenden Informations- und Auskunftsrechte in Art 10–12 der RL. Im Sinne der RL müßte der Anwender dem Speichern des Cookies in seinem PC zustimmen. Aber das kann er gar nicht. Tatsächlich können erst die neueren Versionen der Browser-Software überhaupt so konfiguriert werden, daß sie den Anwender vor dem Speichern eines Cookies warnen. Allerdings müssen, und auch das verstößt gegen die RL, die Browser erst speziell eingestellt werden, damit diese Warnung aktiviert ist.[16])

Auch enthalten derartige Warnungen nicht die in der RL vorgeschriebenen Informationen, damit der Anwender in vollem Wissen der Konsequenzen seine Einwilligung geben kann. Die angezeigten Texte sind vielfach irreführend. Sie kommunizieren nicht, daß, sobald das Cookie gespeichert wurde, es für die Web-Anbieter frei zugänglich ist. Ob der Anwender diesen Zugriffen und nicht nur der Speicherung zustimmen will, bleibt ungeklärt und eröffnet weitere Problemfelder. Ist das Cookie erst gespeichert, bleibt es im Computer des Anwenders. Selbst wenn der Anwender dem Speichern des Cookies zustimmte, hat er ein Recht auf Auskunft über die im Cookie gespeicherten persönlichen Daten. Cookies aber können durch den Anwender – mit Ausnahme der allerneuesten Version mancher Browser – nicht einfach eingesehen werden.

6. Haftung

Nach der RL ist der „für die Verarbeitung Verantwortliche" haftbar für die Einhaltung der Datenschutzbestimmungen bei der Verarbeitung der persönlichen Daten.[17]) Auf dem WWW wird das in den meisten Fällen der Inhalteanbieter (Content-Provider) sein, der über den Web-Server die Cookies erstellt und abfragt. Daher haftet er auch für durch die Verwendung von Cookies erfolgte Verstöße gegen die bestehenden Datenschutzbestimmungen. Betroffene könnten ihn bei den nationalen Gerichten auf Schadenersatz klagen. Art 23 Abs 2 RL legt dabei die Last des Beweises nicht unerheblich auf die Schultern des Verarbeiters.

Jeder Betreiber eines Web-Servers mit illegaler Cookie-Anwendung riskiert daher haftbar gemacht zu werden. Davon besonders betroffen sind nicht nur europäische, sondern auch amerikanische multinationale Unternehmen, die derartige Web-Server in vielen europäischen Ländern betreiben. Weil ihre Web-Server jedenfalls teilweise in Europa liegen, sind die nationalen Datenschutzbestimmungen direkt auf sie anwendbar, und die Verarbeitung muß zu jeder Zeit diesen Normen entsprechend ablaufen.

Die Situation ist freilich grundlegend diffiziler, wenn der Web-Server und der „verantwortliche Verarbeiter" sich in einem Land außerhalb der EU und ohne „adäquaten" Datenschutz befinden. Die Datenschutzbestimmungen, besonders jene auf Übermittlung in Drittländer, sind dann zwar anwendbar, und ihre Verletzung löst die gesetzliche Haftung aus. Die Durchsetzung dieser Betroffenenrechte mag sich vor

12) Art 7 RL.
13) Art 8 RL.
14) Abschnitte IV–VII, Art 10–15 RL.
15) *Netscape,* Persistent Client State HTTP Cookies, Preliminary Specifications, sowie *Kristol/Montulli,* HTTP State Management Mechanism.
16) Kostenlose Software zur Kontrolle von Cookies ist ebenfalls am Internet verfügbar, etwa: Cookie Terminator, Cookie Pal, Cookie Cutter oder Cookie Crusher, http://www.zdnet.com/swlib/internet.html. Eine Anleitung zum Deaktivieren bzw Filtern von Cookies bietet: www.ibm.com/privacy/cookies.html.
17) Art 23 RL.

den nationalen europäischen Gerichten freilich als schwierig erweisen.[18])

Ein anderer Ansatz mag sein, die Hersteller der Software verantwortlich zu machen, die den datenschutzrechtswidrigen Austausch von Cookies überhaupt erst ermöglicht. Denn diese Software-Hersteller haben ihre Software eben unter teilweise bewußter Mißachtung der internationalen Cookies-Standards so entwickelt, daß die hier dargestellte intransparente und damit rechtswidrige Informationsweitergabe möglich wird. Davon umfaßt wären beispielsweise die Browser-Software von Microsoft und Netscape, aber auch die sog Web-Server-Software von Microsoft.

7. Zusammenfassung

Informations-Anbieter innerhalb der Europäischen Union müssen – wenn sie Cookies verwenden – auf die Einhaltung datenschutzrechtlicher Bestimmungen achten, wollen sie nicht geltendes europäisches Datenschutzrecht verletzen. Da die Durchsetzung der Datenschutzrechte gegenüber Providern, die sich außerhalb der Grenzen der Europäischen Union befinden, äußerst schwierig ist, könnten Datenschutzbehörden bei den Herstellern bzw Importeuren der Browser-Software ansetzen und diese zur Verantwortung ziehen.

Die rechtlichen Rahmenbedingungen gelten nicht nur für Cookies, sondern für jede Art von TGI, wie etwa auch Intels CPU-ID.

Den Anwendern ist zu raten, ihre Browser-Software so einzustellen, daß Cookies gar nicht oder nur mit ihrer Zustimmung abgespeichert werden.[19]) Darüber hinaus stehen ihnen die in Österreich verfassungsrechtlich garantierten Rechte auf Geheimhaltung, Auskunft, Richtigstellung und Löschung auch in bezug auf personenbezogene Informationen in Cookies zu.

18) Vgl *Brandl/Mayer-Schönberger,* Wer hat Recht am Infohighway, in Fuglewicz (Hrsg), Das Internet-Lesebuch (1996) 153ff.
19) Vgl dazu die Hinweise in www.ibm.com/privacy/cookies.html.