e-Discovery in Germany?

Von Rechtsanwalt Dr. Michael Rath, Köln, und Saskia Klug, LL.M., Hannover

Mehr über die Autoren erfahren Sie auf S. VIII.

Im Fall einer rechtlichen Auseinandersetzung in den USA (oder etwa Großbritannien) können auch Unternehmen in Deutschland aufgrund von sogenannten „Electronic Discovery"-Regelungen gezwungen sein, kurzfristig elektronisch gespeicherte Informationen („Electronically Stored Information", kurz „ESI") zu reproduzieren, wenn diese zur Sachverhaltsaufklärung oder als Beweismittel in einem Gerichtsverfahren in Betracht kommen. Diese Vorlagepflicht kann erhebliche Ausmaße annehmen. Die Nichteinhaltung der e-Discovery-Bestimmungen kann jedoch (jedenfalls für die Prozesspartei in den USA) zu harten Sanktionen führen. Aus deutscher Sicht stellt sich die Frage, ob eine solch weitreichende Pflicht des „Common Law" zur Datenauswertung und -weitergabe mit hiesigem Recht, insbesondere dem Datenschutzrecht, vereinbar ist. Nachfolgend wird zunächst das US-amerikanische e-Discovery-Verfahren kurz dargestellt (Ziffer I.). Danach wird unter Ziffer II. die Pflicht deutscher Unternehmen zur Mitwirkung an diesen Verfahren untersucht. Hierauf folgt die Erörterung von Möglichkeiten zur Aufbereitung und Herausgabe von Daten im Rahmen einer e-Discovery nach deutschem Recht (Ziffer III.). Unter Ziffer IV. wird dann der Frage nachgegangen, ob und wie US-amerikanisches und deutsches (Datenschutz-) Recht zumindest im Ansatz miteinander in Einklang zu bringen sind.

I. Das e-Discovery-Verfahren in den USA

E-Discovery findet vor allem im Rahmen einer US-amerikanischen „Pre-Trial-Discovery" statt.[1] Dieses gerichtliche Vorverfahren dient der Sachverhaltsfeststellung oder auch der Beweisermittlung und wird weitgehend durch die Parteien ohne Mitwirkung der Richter abgewickelt.[2] In diesem Verfahren können die Parteien gem. Regel 26 (b) (1) der Federal Rules of Civil Procedure (FRCP) von der Gegenseite die Vorlage umfassender Informationen zu allen Tatsachen einfordern, die für den behaupteten Klageanspruch oder die Verteidigung „relevant" sein können.[3] Als relevant stuft die US-amerikanische Zivilprozessordnung dabei auch solche Informationen ein, die zur Auffindung verwertbarer Beweismittel beitragen können, auch wenn diese Vorgehensweise faktisch zu einer Art „Ausforschung" führt.[4] Zudem ist noch nicht einmal ein schlüssiger Vortrag erforderlich, da die Pre-Trial-Discovery erst zur Ermittlung des Sachverhalts führen soll.[5] Diese Informationsanforderung erfolgt in der Praxis durch „written interrogatories", also schriftliche Fragen an die Gegenseite, die gerichtliche „discovery order" oder einen „request for the production of documents", also die anwaltliche Aufforderung an die Gegenseite, relevante Dokumente und Unterlagen aufzubereiten und vorzulegen.[6] Seit dem 1. 12. 2006 fallen gemäß Regel 34 (a) FRCP auch elektronisch generierte und gespeicherte Daten („Electronically Stored Information", ESI) in den Anwendungsbereich der Vorschriften der Pre-trial-Discovery. Hierfür hat sich der Begriff e-Discovery etabliert.

1. Nach dem FRCP vorzulegende Dokumente

Nicht nur die zuvor diskutierte „Relevanz", sondern auch der Begriff „Dokumente" wird im US-amerikanischen Recht weit verstanden. Gemäß Regel 34 (a) FRCP gehören zu den ESI (und damit vorlagepflichtigen Informationen) neben Texten auch Zeichnungen, Grafiken, Tabellen, Fotos, Tonbandaufzeichnungen, Bilder und andere Daten oder Datensammlungen.[7] Zudem geht es nicht nur um die Endfassungen der vorgenannten Dokumente; vielmehr sind auch alle Entwürfe, Anmerkungen und Notizen zu diesen Dokumenten sowie ggfls. unterschiedliche Bearbeiterversionen von der e-Discovery umfasst.[8] Zu den vorlagepflichtigen ESI gehören – mangels anderweitiger Vereinbarung mit den Prozessgegner – schließlich auch die Metadaten, also alle Zusatzinformationen zu den Dokumenten wie Name des Bearbeiters, Datum der Erstellung und der letzten Änderung, etc.[9]

2. Litigation Hold

Eine unabdingbare Aufbewahrungspflicht besteht für diese elektronischen Dokumente, sobald die (spätere) Prozesspartei Kenntnis von dem bevorstehenden Rechtsstreit hat oder hätte haben müssen.[10] Positive Kenntnis liegt jedenfalls ab Zustellung einer Klage vor; vorhersehbar ist aber ein Rechtsstreit z. B. auch schon dann, wenn die Gegenseite eine entsprechende Aufforderung („preservation letter") versandt hat.[11] Spätestens mit Zugang dieser Benachrichtigung besteht für das Unternehmen die Pflicht zur Einrichtung eines „Litigation Hold", d. h. der unternehmensweiten Durchsetzung des Verbotes der Löschung von eventuell beweiserheblichem Material.[12] Natürlich können bei der Verwendung eines in der Regel automatisch ablaufenden Datensicherungsprogramms im Unternehmen auch beweisrelevante Daten verloren gehen. Um die durchaus gravierenden Folgen einer ungewollten Beweisvernichtung einzuschränken, sieht Regel 37 (e) FRCP vor, dass keine prozessuale Sanktionen gegen eine Partei verhängt werden können, wenn der Verlust der Daten das Ergebnis einer „routine, good-faith operation of an electronic information system" war (vgl. hierzu noch nachfolgend).

1 Auch in Großbritannien gibt es vergleichbare e-Disclosure-Bestimmungen (Civil Procedure Rules Part 31), die jedoch vorliegend nicht dargestellt werden sollen.
2 Vgl. etwa *Bolthausen*, MDR 2006, 1081, 1081; *Hess*, AG 2005, 897, 903. Vgl. zum gesamten Thema auch *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008.
3 Siehe *Klinger*, RIW 2007, 108, 108; *Hilgard*, ZIP 2007, 985, 989.
4 *Rath*, ComplianceReport 6/2008, 4, 5.
5 *Geimer*, Internationales Zivilprozessrecht, 5. Aufl. 2005, Rn. 88.
6 Vgl. *Geimer* (Fn. 6), Rn. 89; *Rath* (Fn. 5), 5; *Klinger*, RIW 2007, 108.
7 Vgl. auch *Hilgard*, SchiedsVZ 2008, 122, 123.
8 So auch in Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003).
9 *Klinger*, RIW 2007, 108, 109; *Rath*, ComplianceReport 6/2008, 4, 5.
10 Siehe Fujitsu Ltd. v. Federal Express Corp. 247 F.3d 423, 436 (2nd Cir. 2001).
11 Ebenso *Klinger*, RIW 2007, 108, 111.
12 *Spies/Schröder*, MMR 2008, 275, 275.

3. Sanktionen bei Verstoß gegen die Vorlagepflicht

Die Nichteinhaltung einer „discovery order" kann nach der „doctrine of spoliation" zu erheblichen Sanktionen für die am Prozess beteiligte Konzerngesellschaft führen.[13] Als Sanktionen kommen – zumindest in den USA – der Ausschluss eigener Beweismittel zu einem bestimmten Beweisthema, eine Art Beweislastumkehr und sogar ein Urteil zu Lasten der gegen die Vorlagepflicht verstoßenden Partei in Betracht.[14] Zudem kann der vorlagepflichtigen Partei die Zahlung einer nicht unerheblichen Geldbuße auferlegt werden.[15] Selbst Haftstrafen sind in den USA denkbar.

II. Die Pflicht deutscher Unternehmen zur Mitwirkung

Die zuvor skizzierte Pflicht zur Offenlegung relevanter Dokumente und elektronischer Daten erstreckt sich zunächst nur auf diejenigen Informationen, die sich im Besitz der in den USA klagenden bzw. verklagten Parteien befinden. Nach Regel 34 (a) FRCP ist eine Prozesspartei in den USA aber nicht nur zur Herausgabe derjenigen für einen Prozess relevanten Unterlagen verpflichtet, die sie in direktem Besitz hat, sondern muss alle Unterlagen vorlegen, die sich in Besitz, Verwahrung oder unter der Kontrolle der Partei, von der die Vorlage verlangt wird, befinden („in the party's possession, custody or control"). Durch das letztgenannte Merkmal („control") kann eine Offenlegungspflicht auch solche Dokumente betreffen, die sich im Besitz einer (deutschen) Konzerngesellschaft befinden, selbst wenn diese gar nicht direkt am Verfahren beteiligt ist. Dies soll nach US-amerikanischem Prozessverständnis sogar dann gelten, wenn die Partei nur rein tatsächlich die Möglichkeit hat, die Dokumente zu erlangen.[16] Damit können die Anforderungen von e-Discovery faktisch auch deutsche Unternehmen betreffen, wenn sie z. B. ein Tochterunternehmen eines amerikanischen Konzerns sind („alter ego theory") oder selbst in den USA Geschäftstätigkeit entfalten („doing business", „minimum contacts").

Trotz dieser ausufernden Bejahung US-amerikanischer Gerichtszuständigkeit ist es für die das Verfahren in den USA betreibende Partei verfahrensrechtlich kaum möglich, eine deutsche Gesellschaft unmittelbar prozessual zu verpflichten. Verfahrenstechnisch käme hier etwa ein Amtshilfeersuchen zur Durchführung eines Beweisverfahrens nach dem Haager Übereinkommen über die Beweisaufnahme im Ausland in Betracht. Zudem wäre denkbar, ein deutsches Unternehmen unmittelbar prozessual zu verpflichten, was dann allerdings auch Fragen der Zustellung nach dem Haager Übereinkommen aufwirft.

1. Das Haager Übereinkommen über die Beweisaufnahme im Ausland

Nach dem Haager Übereinkommen über die Beweisaufnahme im Ausland (HBÜ) vom 1. 3. 1970[17], zu dessen Vertragsstaaten sowohl Deutschland als auch die USA[18] zählen, erfolgt eine Beweisaufnahme im Ausland grundsätzlich nach dem jeweiligen ausländischen Recht durch die ausländischen Behörden.[19] Bezüglich der Ersuchen im Rahmen einer Pre-Trial-Discovery hat Deutschland gemäß Art. 23 HBÜ einen Vorbehalt dahingehend erhoben, Rechtshilfeersuchen, die ein Verfahren zum Gegenstand haben, das in den Ländern des „Common Law" unter der Bezeichnung „pre-trial discovery of documents" bekannt ist, nicht zu erledigen.[20] Die vorgenannte Beschränkung auf die „Pre-Trial-Discovery of Documents" wirft allerdings die Frage auf, ob damit der Vorbehalt auch für die e-Discovery gilt, da „documents" und „electronically stored information" (ESI) im FRCP nicht gleichgesetzt werden.[21] Für eine Zeugenvernehmung gilt der Vorbehalt jedenfalls nicht.[22] Unbestreitbar sind ESI aber Dokumenten ähnlicher als etwa die Zeugenvernehmung. Zudem gab es zum Zeitpunkt der Unterzeichnung des HBÜ und der Erklärung des Vorbehalts durch Deutschland noch gar keine e-Discovery im eingangs definierten Sinn. Auch vor der Änderung der Regel 34 (a) FRCP im Dezember 2006 wurden elektronisch generierte Daten unter den Begriff „Document" subsumiert.[23] Eine Klarstellung und Ergänzung in einem US-amerikanischen Gesetz wie dem FRCP kann aber schwerlich zu einer Begrenzung des von der Bundesrepublik Deutschland erklärten Vorbehalts führen, so dass im Ergebnis auch die Herausgabe von ESI dem Vorbehalt gem. Art. 23 HBÜ unterfällt. Die Durchführung einer e-Discovery mit Hilfe der deutschen Gerichte ist damit ausgeschlossen.

2. Direkte Verpflichtung der Unternehmen

Der Ausschluss der e-Discovery über das HBÜ schließt allerdings – zumindest aus Sicht der US-amerikanischen Gerichte – nur die Beweiserhebung mit Hilfe der deutschen Behörden, nicht aber die direkte Inanspruchnahme der ausländischen Unternehmen zur Vorlage von ESI aus. Denn die US-amerikanischen Gerichte sehen die Regelungen des HBÜ nicht als zwingend an und wenden daher die Regelungen des FRCP trotz des Vorbehaltes im HBÜ an.[24] Zudem zeigen die US-Gerichte bekanntlich die Neigung, auch für grenzüberschreitende Sachverhalte die eigene Zuständigkeit („jurisdiction") zu bejahen.[25] Soweit also die Beweisaufnahme in den USA stattfinden soll und sich lediglich die dafür vorzulegenden Dokumente in einem anderen Staat befinden, wenden US-amerikanische Gerichte oft die Regelungen des FRCP ohne Beschränkung an.[26] Diese Anordnung durch US-Gerichte ist zwar im (deutschen) Ausland nicht unmittelbar vollstreckbar.[27] In der Praxis befolgen jedoch viele deut-

13 „Spoliation" bedeutet die „Vernichtung, Veränderung, Verheimlichung oder Unterdrückung von Beweismitteln, die ein anderer in einem anhängigen oder vernünftigerweise vorhersehbaren Rechtsstreit benötigt, siehe auch *Klinger*, RIW 2007, 108, 110.
14 *Rath* (Fn. 5), 4, 5.
15 *Klinger*, RIW 2007, 108, 110.
16 *Bolthausen*, MDR 2006, 1081, 1081; *Klinger*, RIW 2007, 108,109.
17 BGBl II, 1977, Nr. 54, S. 1472 ff.
18 BGBl II, 1979, Nr. 30, S. 780 f.; BGBl II, 1980, Nr. 40, S. 1290 ff.
19 Siehe hierzu insbesondere *Bolthausen*, MDR 2006, 1081, 1082.
20 § 14 Abs. 1 Gesetz zur Ausführung des Haager Übereinkommens vom 15. 11. 1965 über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke im Ausland in Zivil- oder Handelssachen und des Haager Übereinkommens vom 18. 3. 1970 über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen vom 22. 12. 1977 (BGBl. I S. 3105).
21 So auch *Spies*, MMR 7/2007, V, VI.
22 Vgl. zuletzt OLG Celle, Beschl. v. 6. 7. 2007 – 16 VA 5/07, NJW-RR 2008, 79.
23 Siehe hierzu Zubulake v. Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003).
24 Société Nationale Industrielle Aérospatiale v. U.S. District Court (8th Cir.) 55 LW 4842 – 4855 (1987), JZ 1987, 984; *Bolthausen*, MDR 2006, 1081, 1083; *Trittmann/Leitzen*, IPRax 2003, 7, 8; *Schack*, Internationales Zivilverfahrensrecht, 4. Aufl. 2006, Rn. 403.
25 *Trittmann/Leitzen*, IPrax 2003, 7, 7; *Schütze*, RIW 2005, 579, 582 ff.
26 *Wazlawik*, IPRax 2004, 396, 397; *Schack* (Fn. 25), Rn. 734.
27 *Wazlawik*, IPRax 2004, 396, 397.

sche Unternehmen diese Weisungen der (für sie zumindest nach deutschem Recht unzuständigen) Gerichte auch ohne drohende Zwangsmaßnahmen – entweder aus Kostengründen, zur Vermeidung von Sanktionen oder weil sie selbst Interesse an der Durchführung der Pre-Trial-Discovery haben.[28]

III. Das Recht zur Aufbewahrung und Herausgabe aus deutscher Sicht

Vorlagepflichten in dem zuvor geschilderten Ausmaß sind dem deutschen Recht fremd.[29] Aufbewahrungspflichten für Dokumente und Daten finden sich nur vereinzelt, so z. B. in § 257 HGB oder § 147 AO.[30] Allgemein gültige und nur auf das (digitale) Format bezogene Vorgaben zur Speicherung und Aufbereitung digitaler Informationen gibt es im deutschen Recht nicht; sie lassen sich nur aus den allgemein gültigen Grundsätzen ableiten.[31] Angesichts der zuvor dargestellten Reaktionen deutscher Unternehmen stellt sich jedoch die Frage der Zulässigkeit der Aufbereitung und Herausgabe der im Rahmen einer e-Discovery angeforderten Daten nach deutschem (Datenschutz-) Recht.

1. Datenschutzrecht des BDSG als Schranke der zulässigen Datenverarbeitung

Das deutsche Datenschutzrecht findet gem. § 1 Abs. 5 BDSG für alle im Inland erhobenen personenbezogenen Daten Anwendung und erfasst daher auch die Erhebung und Übermittlung dieser Daten ins Ausland im Rahmen einer e-Discovery. Das BDSG basiert bekanntlich gem. § 3 a BDSG auf den Grundsätzen der Datenvermeidung und Datensparsamkeit, d. h., es sollen so wenig wie möglich personenbezogene Daten erhoben und gespeichert werden. Daher ist zumindest nach deutschem Datenschutzrecht sowohl die Aufbewahrung (Speicherung) als auch die Aufbereitung und Herausgabe von Daten im Rahmen einer e-Discovery nur unter eng begrenzten Voraussetzungen möglich.

a) Speicherung von personenbezogenen Daten

Die Erhebung, Speicherung und Übermittlung von personenbezogenen Daten ist nur in den engen Grenzen des § 28 BDSG zulässig. Im Hinblick auf den zuvor dargestellten Umfang der Datenerhebung bei einer e-Discovery ist es jedoch unvermeidbar, dass hiervon (vor allem bei E-Mails) auch personenbezogene Daten i. S. d. BDSG betroffen sind. Datenerhebung und -speicherung zu Zwecken einer eventuellen Herausgabepflicht im Rahmen einer e-Discovery können allerdings gem. § 28 Abs. 1 Nr. 2 BDSG zu rechtfertigen sein, soweit diese zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Grundsätzlich ist ein solches Interesse bei der Verteidigung von Rechtsansprüchen gegeben.[32] Obwohl dies grundsätzlich auch für die Rechtsdurchsetzung im Ausland gelten muss, wird hierdurch jedoch nicht jede durch ein ausländisches Gesetz oder Gericht geforderte Datenspeicherung legitimiert, da sonst jederzeit das deutsche bzw. europäische Recht unterlaufen werden könnte.[33] Nur wenn ein Unternehmen ausreichende Vorkehrungen, z. B. durch eine sog. „Document Retention Policy" trifft, um einerseits die notwendigen Dateien zu speichern, und andererseits den Grundsätzen des Datenschutzes Rechnung zu tragen, kommt also überhaupt eine Rechtfertigung der Erhebung und Speicherung der Daten gem. § 28 Abs. 1 Nr. 2 BDSG in Betracht. Zusätzlich ist aber immer noch eine Interessenabwägung erforderlich, so dass die Zulässigkeit der Verarbeitung der Daten gem. § 28 Abs. 1 Nr. 2 BDSG für jeden Einzelfall der e-Discovery konkret zu ermitteln ist. Nach deutschem Verständnis des Datenschutzes wird insbesondere angesichts des zuvor erwähnten Grundsatzes der Datensparsamkeit diese Interessenabwägung oftmals gegen die Zulässigkeit einer e-Discovery-Maßnahme sprechen.

b) Übermittlung der Daten in die USA

Hinzu kommen die Schwierigkeiten bei der Rechtfertigung der Übermittlung der relevanten ESI in die USA. Grundsätzlich lässt sich zwar auch diese Übermittlung von Daten nach § 28 Abs. 1 Nr. 2 BDSG rechtfertigen. Dies gilt aber nicht bei grenzüberschreitenden Datenübermittlungen gem. § 4 b Abs. 2 S. 2 BDSG, wenn in dem Staat, in den die Daten übermittelt werden sollen, ein angemessenes Datenschutzniveau nicht gewährleistet ist, was in den USA der Fall ist. Zwar sieht § 4 c Abs. 1 S. 1 Nr. 4 BDSG auch in einem solchen Fall vor, dass die Verteidigung von Rechtsansprüchen vor Gericht die Übermittlung rechtfertigen kann, jedoch unterliegen die übermittelten Daten dann gem. § 4 c Abs. 1 S. 2 BDSG einer Zweckbindung: Ihre Verwendung ist ausschließlich zu dem Zweck zulässig, zu dessen Erfüllung sie übermittelt wurden, im Rahmen einer e-Discovery also nur zu Verfahrenszwecken. Für US-Verfahren gilt allerdings der Grundsatz, dass eingebrachte Dokumente auf Antrag der Öffentlichkeit zugänglich zu machen sind.[34] Da dies in deutlichem Widerspruch zu den Anforderungen der §§ 4 b, 4 c BDSG steht, kann zumindest die uneingeschränkte Übermittlung von personenbezogenen Daten im Rahmen einer e-Discovery nicht mit dem deutschen Datenschutzrecht in Einklang gebracht werden.

2. Schutz des Fernmeldegeheimnisses

Die Situation verkompliziert sich noch weiter, wenn in dem betreffenden Unternehmen die private Internetnutzung erlaubt ist oder toleriert wird. In diesem Fall wird der Arbeitgeber, also das Unternehmen, bekanntlich wie ein Anbieter von Telekommunikationsdiensten i. S. d. § 3 Nr. 6, 10 TKG behandelt, und ist daher u. a. zum Schutz des Fernmeldegeheimnisses nach § 88 TKG verpflichtet.[35] Danach unterliegen Inhalte der Telekommu-

28 So auch *Spies*, MMR 7/2007, V, VI; *Hilgard*, ZIP 2007, 985, 990.
29 Allein ein E-Mail-Archiv eines einzigen Mitarbeiters mit nur 1 GB bedeutet rund 9000 E-Mails mit ca. 3000 Anhängen; ausgedruckt entspräche dies ca. 75 000 Seiten DIN A4.
30 *Hilgard*, ZIP 2007, 985, 986.
31 *Rath*, in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, 5, 15.
32 *Spies/Schröder*, MMR 2008, 275, 278.
33 Mit dieser Begründung hat bereits die Art.29-Datenschutzgruppe der EU in der Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität v. 1. Februar 2006 die den Unternehmen nach dem US-amerikanischen Sarbanes-Oxley Act (SOX) auferlegten Verpflichtungen nicht als Grundlage einer Rechtfertigung der Datenspeicherung gem. Art. 7 c) der Richtlinie 95/46/EG angesehen.
34 *Spies/Schröder*, MMR 2008, 275, 279.
35 *Eckhardt*, in: Heun, Handbuch Telekommunikationsrecht, 2. Aufl. 2007 Rn. L 76; *Härting*, ITRB 2008, 88, 88 f.; *Rath/Karner*, K&R 2007, 446, 447.

nikation dem Fernmeldegeheimnis, ebenso wie die dazugehörigen Bestandsdaten.[36] Besonders problematisch ist dann die Übermittlung von Telekommunikationsdaten ins Ausland. Denn gemäß § 92 TKG dürfen Daten – in Ergänzung zu den Regelungen des BDSG – nur dann übermittelt werden, soweit dies für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Missbrauchsbekämpfung erforderlich ist. In § 92 TKG findet sich also die Legitimation der Übermittlung zu Zwecken der Rechtsverfolgung nicht wieder. Eine Rechtfertigung der Übermittlung von „Telekommunikationsdaten" in die USA aufgrund der Vorlagepflicht im Rahmen einer e-Discovery scheidet damit aus, soweit die Vorschriften des TKG Anwendung finden.

3. Beteiligungsrechte des Betriebsrates

Oft wird zudem übersehen, dass der Betriebsrat – soweit ein solcher in dem betreffenden Unternehmen besteht – gem. § 87 Nr. 6 BetrVG Mitbestimmungsrechte bezüglich des Umgangs mit E-Mail und der Internetnutzung hat.[37] So stehen dem Betriebsrat z. B. Mitbestimmungsrechte bezüglich der Datenerhebung und -verwendung zu.[38] Auch eine Übermittlung der Daten in die USA wäre daher mit dem Betriebsrat abzustimmen. Hier ist in der Praxis regelmäßig mit erheblichem Diskussionsbedarf zu rechnen, zumindest wenn der Betriebsrat nicht frühzeitig in das e-Discovery-Verfahren einbezogen wird.

4. Zwischenergebnis

Nach deutschem Datenschutz- und Telekommunikationsrecht ist es nach dem Vorgesagten schwierig, die Speicherung und Übermittlung von ESI, wie sie bei einer e-Discovery nach US-amerikanischem Recht notwendig sind, zu rechtfertigen. Denn das strenge deutsche Datenschutzrecht steht in deutlichem Gegensatz zu den weitreichenden Verpflichtungen des US-amerikanischen FRCP.

IV. Ein unlösbarer Gegensatz?

Deutsches Datenschutzrecht und US-amerikanisches Prozessrecht scheinen damit zunächst unvereinbar. Dies ist auch verständlich, ist doch der Begriff des „Datenschutzes" in Europa kaum mit dem angloamerikanischen Verständnis von „data protection" in Einklang zu bringen, da dieser Terminus in den USA vorwiegend die physische Sicherheit der Daten beschreibt. Zudem wird der Schutz der Privatsphäre („privacy") lediglich unter dem Gesichtspunkt des Schutzes vor staatlichen Eingriffen erörtert, eine diesbezügliche Verpflichtung Privater ist dem US-amerikanischen Recht fremd. Für die im Rahmen einer e-Discovery regelmäßig stattfindenden Verhandlungen nach Regel 408 FRCP („meet & confer") kann möglicherweise bereits die Pseudonymisierung der zu übermittelnden Daten ein Ausweg aus diesem datenschutzrechtlichen Dilemma sein. Daneben kann die rein rechtliche Lösung des Problems – wenn sich deutsche Unternehmen der e-Discovery aus den zuvor genannten Gründen nicht verweigern wollen – wohl nur im Rahmen des US-amerikanischen Gerichtsprozesses gesucht werden. Denn neben im Ergebnis kaum zielführenden Maßnahmen wie die Hinterlegung von Schutzschriften unter Berufung auf die vorgenannten Haager Übereinkommen sowie die Erhebung einer negativen Feststellungsklage zwecks Begründung anderweitiger Rechtshängigkeit („German Torpedo") kommt trotz dieser Gegensätze auch und gerade die Berufung der vorlagepflichtigen Partei auf das ausländische (deutsche) Datenschutzrecht in Betracht.

1. Berufung auf deutsches Datenschutzrecht im e-Discovery Verfahren

Grundsätzlich kann eine Prozesspartei von ihrer Verpflichtung zur Vorlage von Papierdokumenten oder ESI befreit werden, wenn dieser ein ausländisches Gesetz, zu dessen Einhaltung die Partei verpflichtet ist, entgegensteht. Dass dies – zumindest derzeit – aber nur mit erheblichem Begründungsaufwand und ungewissen Erfolgsaussichten möglich ist, zeigt eine Entscheidung des US District Court of California vom 19. 5. 2007.[39] In diesem Verfahren verlangte Columbia Pictures von den Betreibern der Website „Torrent Spy" die Vorlage von Server-Log Dateien, insbesondere der IP-Adressen der Nutzer der Webseite. Dies sollte helfen, den illegalen Download von Filmen mit Hilfe der Software „Torrent Spy" zu beweisen. Die Betreiber verweigerten die Herausgabe unter anderem mit Hinweis auf das für sie geltende (niederländische) Datenschutzrecht, nach welchem eine solche Übermittlung verboten sei. Das Gericht setzte sich über diese Einwände hinweg und gab dem Verlangen nach einem Transfer der Daten statt. Zum einen sah es das US-Gericht nicht als erwiesen an, dass die Vorlage von Server-Log-Dateien tatsächlich unter niederländisches Datenschutzrecht falle, da diese nur für personenbezogene Daten gelte und eine IP-Adresse einen Computer, nicht aber eine spezielle Person identifiziere. Des weiteren sah das Gericht das niederländische Datenschutzrecht als sog. „blocking statute" an. Nach US-amerikanischem Recht berechtigt dieses Rechtsinstitut das Gericht, sich über entgegenstehende Gesetze hinwegzusetzen, wenn eine Abwägung der betroffenen Interessen zugunsten des Interesses an der Rechtsverfolgung ausfällt. In die Abwägung wurden vom Gericht die Bedeutung der Unterlagen für den Rechtsstreit, die Genauigkeit, mit der die verlangten Unterlagen bezeichnet werden, die Herkunft der Daten, die Verfügbarkeit alternativer Methoden der Informationsgewinnung, die Interessen der USA bzw. des ausländischen Staates und der Aufwand, der für die Informationsbeschaffung erforderlich wäre, einbezogen.[40] Im vorliegenden Fall fiel die Abwägung vor allem deswegen zu Lasten der Betreiber der Webseite aus, weil diese sich nach Ansicht des Gerichts den Server in den Niederlanden gerade im Hinblick auf das dort geltende Datenschutzrecht ausgesucht hätten.[41]

Diese Interessenabwägung könnte künftig anders ausfallen: Da in der Vergangenheit datenschutzrechtliche Verstöße in Deutschland kaum geahndet wurden, erkennen

36 *Bock*, in: Geppert, Beck'scher TKG Kommentar, 3. Aufl. 2006, § 88 Rn. 11, 13.
37 *Hilgard*, ZIP 2007, 985, 991; *Rath/Karner*, K&R 2007, 446, 448.
38 *Klebe*, in: Däubler/Kittner/Klebe, BetrVG, 11. Aufl. 2008, § 87 Rn. 158.
39 Columbia Pictures Industries v. Justin Bunnell, No. CV 06-1093 FMC(JCx).
40 Columbia Pictures Industries v. Justin Bunnell, No. CV 06-1093 FMC(JCx), S. 29 der Urteilsgründe.
41 Columbia Pictures Industries v. Justin Bunnell, No. CV 06-1093 FMC(JCx), S. 30 der Urteilsgründe.

US-Gerichte die „Ernsthaftigkeit“ der entgegenstehenden Datenschutzrechte nur sehr eingeschränkt an. Sobald auch hier in Deutschland – erste Tendenzen sind ja durchaus zu erkennen – strengere Sanktionen bei Verstößen gegen das BDSG zu befürchten sind, könnte sich auch die Meinung der US-Richter diesbezüglich ändern.

2. Beantragung einer „protective order“

Eine Alternative zur Verweigerung der Vorlage von Unterlagen unter Berufung auf das deutsche Datenschutzrecht ist die Beantragung einer „protective order“ gem. Regel 26 (c) FRCP.[42] Danach kann das Gericht die Vorlagepflicht bei Vorliegen wichtiger Gründe („good cause“) einschränken, um die Partei vor unangemessenen Belastungen („undue burden“) zu schützen. In Betracht kommt hierbei z. B. das Verbot, die vorgelegten Daten zu veröffentlichen oder die Übergabe derselben in einem versiegelten Umschlag an das Gericht. Denkbar wäre auch die Verabredung eines „Attorneys-Eyes-Only“-Privilegs im Rahmen des „meet & confer“. Allerdings liegt – sofern diese Einschränkungen nicht im Verhandlungswege erreicht werden können – die Gewährung des Schutzes immer im Ermessen der Gerichte, welche diesen bislang eher eng bemessen.[43]

3. Mögliche Vorsorgemaßnahmen

Bis zu einer (datenschutz-) rechtlichen Lösung des Problems der gegensätzlichen Anforderungen im deutschen und US-amerikanischen Recht bleibt Unternehmen mit Geschäftstätigkeit in den USA bzw. mit im Ausland ansässigen Konzerngesellschaften nur, im Rahmen ihrer Bemühungen um die Einhaltung von IT-Compliance, entsprechende Prozesse einzuführen, um eine vollständige Aufbewahrung relevanter Dokumente (einschließlich deren Entwürfe und Metadaten) sicherzustellen. Es muss dabei unter Beachtung des geltenden Datenschutzrechtes gewährleistet sein, dass die Vernichtung von relevanten Unterlagen und die Löschung elektronischer Daten konzernweit geregelt ist und spätestens dann ausgesetzt wird, sobald ein Rechtsstreit vorhersehbar wird oder diese Daten anderweitig benötigt werden.

a) Die „Sedona-Principles“

Einen weiteren Anhaltspunkt für den Umgang mit ESI im Hinblick auf ein drohendes e-Discovery-Verfahren in den USA liefern die von der sog. „Sedona Conference“ herausgegebenen „Sedona Principles Addressing Electronic Document Production“.[44] Diese rechtlich nicht bindenden, in den USA aber durchaus anerkannten Prinzipien, beschreiben die Verpflichtungen der Parteien während einer e-Discovery. Bezüglich der Pflicht zur Aufbewahrung von Daten sind insbesondere die Prinzipien Nr. 1, 3, 5, 6, 8, 9 und 12 relevant. Aus diesen ergibt sich, dass von keiner Partei erwartet werden kann, ausnahmslos alle Daten aufzubewahren (Nr. 5) und dass bei einer e-Discovery möglichst darauf verzichtet werden sollte, bereits gelöschte oder noch herzustellende Daten zu verlangen (Nr. 8).

b) „Document Retention Policy“

Zudem kann mit Hilfe einer Unternehmens-Richtlinie für die Archivierung und Löschung von Daten, einer sog. „Document Retention Policy“, der einheitliche Umgang mit elektronischen Daten im Konzern sichergestellt und die unnötige Aufbewahrung oder frühzeitige Löschung von Daten verhindert werden. Eine solche systematische Löschung von Dateien lässt sich dann auch mit dem FRCP in Einklang bringen. Regel 37 (f) FRCP bietet insofern Schutz vor Sanktionen, wenn eine Partei bestimmte ESI nicht beibringen kann, weil sie als Ergebnis einer routinemäßigen, gutgläubigen Handlung in einem elektronischen Informationssystem verloren gegangen sind. Die Ausnahme gilt nicht nur für automatische, sondern auch für manuelle Prozesse und ist nicht an eine bestimmte Praxis der Datensicherung gebunden.[45] Dieser „Safe-Harbor“ gilt jedenfalls dann, wenn die Unternehmensrichtlinie nachvollziehbar ist und die Löschung der Daten nicht einzig dem Zweck dient, Daten einem eventuellen späteren Gegner in einem Prozess vorzuenthalten.[46] Die Einführung einer Document Retention Policy, die sich einerseits am deutschen Datenschutzrecht orientiert und andererseits den Anforderungen der Regel 37 (f) FRCP genügt, erscheint daher ebenfalls als ein Hilfsmittel, den Konflikt zwischen deutschem Datenschutz und amerikanischem Prozessrecht zumindest zu entschärfen.

Hinweis der Redaktion:

Weitere Informationen zum Thema „Electronic Discovery gegen deutsche Unternehmen“ finden Sie im Buch von *Abbo Junker* aus der RIW-Schriftenreihe.

42 *Hess*, AG 2005, 897, 904.
43 Siehe hierzu auch *Hay*, US-Amerikanisches Recht, 3. Aufl. 2005, Rn. 189.
44 www.thesedonaconference.org (Stand: 9. 9. 2008).
45 *Allman*, Northwestern Journal of Technology and Intellectual Property, Vol. 5, No.1 2006, 1, 4/13.
46 *Allman*, Northwestern Journal of Technology and Intellectual Property, Vol. 5, No.1 2006, 1, 17.

Rechtsprechung

Werbe-Anfrage per E-Mail bei Verein unzulässig – FC Troschenreuth

BGH, Urteil vom 17. 7. 2008 – I ZR 197/05

Vorinstanzen: OLG Düsseldorf, 4. 10. 2005 – I-20 U 64/05; LG Kleve, 4. 3. 2005 – 8 O 120/04

§ 7 Abs. 2 Nr. 3 UWG

Gibt ein Sportverein in der Rechtsform des eingetragenen Vereins auf seiner Website eine E-Mail-Adresse an, so liegt darin keine konkludente Einwilligung, gewerbliche Anfragen nach Dienstleistungen des Vereins (hier: Platzierung von Bannerwerbung auf der Website des Vereins) mittels E-Mail zu empfangen. (Leitsatz des Gerichts)