Rezensionen

Rechtsanwalt Dr. Eren Basar, Düsseldorf

Matthias H. Hartmann (Hrsg.): Internationale E–Discovery und Information Governance -

Praxislösungen für Juristen, Unternehmer und IT–Manager

2011, Erich Schmidt Verlag, € 44,95, 318 S.

I. Einleitung zur Problemstellung

Die Beschlagnahme umfangreicher Datensätze wurde in Wirtschaftsstrafverfahren lange Zeit als Wohltat gesehen. Hintergrund war der Blick auf die Alternative: die Beschlagnahme der EDV mit der Folge, dass der Mandant die unternehmenseigene EDV nicht mehr nutzen und die unternehmerische Tätigkeit nicht mehr fortgeführt werden konnte. Mittlerweile sehen sich Verteidiger vielerorts mit dem Problem konfrontiert, dass die Größe der beschlagnahmten Datenmengen - und hier insbesondere der beschlagnahmte Email-Verkehr - kaum noch beherrscht werden kann. Konsequent hat sich ein Markt diverser Anbieter entwickelt, die „E–Discovery"–Tools bewerben, mit denen eine Analyse von größeren Datenmengen erleichtert werden soll. Die vorliegende Monographie beschäftigt sich mit der E–Discovery und dem Information Governance im internationalen Kontext. Der Titel mag auf den ersten Blick kein „klassisches" Thema der Strafverteidigung in Wirtschaftstrafsachen behandeln, doch würde diese Sicht angesichts der beschriebenen Entwicklung zu kurz greifen. Die Erfahrungen mit der „E–Discovery" aus internationalen Rechtsstreitigkeiten können helfen, den Blick für Strategien zur Datenanalyse in Wirtschaftsstrafverfahren zu schärfen. Hinzu kommt, dass der zur Prävention von Strafverfahren beauftragte Unternehmensverteidiger die Fähigkeit des Unternehmens zur Identifizierung, Sicherung und zum Export von Daten in seine Erwägungen einbeziehen muss. Ein Unternehmen, das Ermittlungsbehörden in kürzester Zeit treffsicher Datensätze zur Verfügung stellen kann, kann unter Umständen die Beschlagnahme weitflächiger Datenareale verhindern und somit die Gefahr von Zufallsfunden minimieren.

II. Idee des Buches und grundlegende Ansätze

Die Idee zu dem Buch ist laut dem Herausgeber, *Prof. Dr. Hartmann*, aus einem konkreten E–Discovery-Projekt entstanden. Der Herausgeber selbst lehrt Betriebswirtschaftslehre an der Hochschule für Technik (HTW) in Berlin und war in den Jahren 2007 bis 2009 beurlaubt. In diese Zeit fiel ein Beratungsprojekt, das nach seiner eigenen Aussage die Grundlage des Buches lieferte. Die Autoren verfügen allesamt über „E–Discovery" Erfahrungen aus unterschiedlichen Perspektiven. Diese Streuung ist nicht zufällig. *Hartmann* betont, dass E–Discovery interdisziplinäres Denken von Jurisprudenz, Betriebswirtschaft und Informationstechnologie erfordere (S. V). Weiter sei zu beachten, dass im internationalen Kontext ein Verständnis für die Eigenheiten nationaler Rechtskulturen vorhanden sein müsse. Der Aufbau des Buches folge diesen beiden wichtigen Bausteinen und soll jeweils eine fachliche Perspektive aufbereiten: In Kapitel I geht es um die „E–Discovery im internationalen Rechtsstreit" (Juristische Perspektive), in Kapitel II um „E–Discovery und deutscher Datenschutz" (Datenschutz-Perspektive), in Kapitel III um „E–Discovery und Information Governance" (Betriebswirtschaftliche und technologische Perspektive) und Kapitel IV handelt schließlich von „The Sedona Conference".

III. Die Ausführungen im Einzelnen

Definition von „E-Discovery“

Die Einführung wird von *Prof. Dr. Hartmann* unter dem Titel „Systematische E–Discovery und Information Governance“ (S. 1-20) selbst vorgenommen. Er führt als Folge seiner Projekterfahrung aus, dass E–Discovery mehr ist als eine reine Recherche in Datensätzen: „Informationen mussten identifiziert, in Beziehung gesetzt, aufbereitet und weltweit zur Verfügung gestellt werden. Dieser Vorgang hat einen Namen: E–Discovery“. Im engeren (juristischen) Sinne bedeute E–Discovery die „Offenlegung (Disclosure) von Datenmaterial für eine anstehende gerichtliche Auseinandersetzung“; im weiteren Sinne umfasse E–Discovery auch die informationstechnologische und betriebswirtschaftliche Ebene. Abgegrenzt wird dieser Begriff zugleich von der E–Forensik oder Computer–Forensik. Diese ist ein Mittel, um auch gelöschte Daten oder Dateien wiederherzustellen. Auch wenn diese Begriffe somit nicht deckungsgleich sind, seien sie nicht notwendig gegensätzlich, denn E–Forensik könne ein Mittel der E–Discovery sein (S. 5). Dem pragmatischen Nutzen der E–Discovery für den Auskunftsersuchenden stünden dabei Schutzinteressen der betroffenen Personen oder Unternehmer entgegen – eine Problemlage, die auch in Strafverfahren bei größeren Datenmengen eine Rolle spielt. *Hartmann* weist zutreffend darauf hin, dass die mangelnde Vorbereitung des „Datenhaushaltes“ Kosten in Millionenhöhe nach sich ziehen könne (S. 10), weswegen „E–Discovery-Readiness“ ein wichtiger Baustein von Prävention ist. Immerhin könne in Rechtsstreitigkeiten die ganze Existenz des Unternehmens auf dem Spiel stehen (S. 12). *Hartmann* präsentiert an dieser Stelle auch einen Führungsvorgang einer E–Discovery. Schließlich führt *Hartmann* den Begriff „Information Governance“ ein, bei dem es um nichts anderes als einen „geordneten Informationshaushalt“ oder schlicht um die Frage geht, dass die Informationen und Daten im Unternehmen systematisiert werden mit dem Ziel, jederzeit zu „wissen, was man weiß“. Eine wirksame Information Governance sei somit „conditio sine qua non“ der E–Discovery (S. 16).

Datenschutz im multinationalen Konzern

Rosenthal und *Zeunert* behandeln das Thema „E–Discovery und Datenschutz: Herausforderungen und Lösungsansätze für multinationale Unternehmen“ (S. 23 -71) und zeichnen zunächst das generelle Spannungsfeld bei einer E–Discovery in einem multinationalen Konzern nach: Das Verfahren der Pre–trial Discovery nach US–amerikanischem Vorbild verlange die schonungslose Offenlegung aller im weitesten Sinne für den Fall relevanten Unterlagen – der Datenschutz in Europa schränke eine solche massiv ein (S. 24). Für multinationale Konzerne bestünde dennoch die Pflicht, den Widerspruch zu lösen. Dabei werde der Konflikt durch unterschiedliche Rechtsverständnisse zusätzlich verschärft: Im US–Prozessrecht gingen alle Parteien davon aus, dass jede Partei alle relevanten Daten in ihrem Bereich sicherstelle und allen Beteiligten im Prozess zur Verfügung stelle (Pre-Trial Discovery), während im kontinentaleuropäischen Recht jeder Partei selbst überlassen bleibe, welche Beweismittel sie einbringe (S. 28). *Rosenthal* und *Zeunert* legen dabei dar, dass es bei multinationalen Konzernen fast zwangsläufig zu einem Aufeinanderprallen dieser Verständnisse kommen muss, nämlich wenn die US–Tochter eines europäischen Konzerns Beklagte in einem US – Zivilprozess ist. Dann könne die Pre–Trial Discovery auch Unterlagen in der Konzernzentrale erfassen (S. 29). Allerdings sei der häufigste Konflikt im Datenschutz zu verorten, bei dem multinationale Unternehmen vor fünf rechtlichen Herausforderungen stünden (S. 32 ff.). Diese Herausforderungen begännen bereits in Bezug auf den Geltungsbereich. Das Unternehmen müsse alle Datenschutzbestimmungen der Länder kennen, in denen es operiere. Dies bedeute für die Anwendung, entweder die Datenbestände nach dem jeweiligen Recht zu klassifizieren oder einheitlich den strengsten Schutzstandard anzuwenden. Es ist keine Überraschung, wenn die Autoren darauf hinweisen, dass Letzteres oftmals die vorgezogene Lösung darstellt (S. 34). Weitere Herausforderungen seien die Zweckbindung der erhobenen Daten (und die damit verbundene Frage, ob und unter welchen Voraussetzungen die nachträgliche Umnutzung der Personendaten zulässig ist), die Verhältnismäßigkeit der offenzulegenden Dateien, die Rechte der betroffenen Personen und die grenzüberschreitende Bekanntgabe (S. 36 ff.). Erfreulicherweise belassen *Rosenthal* und *Zeunert* es nicht bei der Beschreibung der Herausforderungen, sondern bieten Lösungsansätze, die in einer aus der Praxis resultierenden Standardprozedur zur Durchführung einer E–Discovery in Europa münden (S. 60).

„E-Discovery-Fähigkeit“

Ebenfalls praktische Hilfestellungen bietet *Murray*, „E-Discovery-Strategien für international agierende Unternehmen“ (S. 74 -81), der in der Neufassung der US-amerikanischen Federal

Rules of civil Procedure (FRCP) mit Wirkung vom 01.12.2006 den Grundstein für mehr und komplexere Rechtsstreitigkeiten sieht. Die in Europa weit verbreitete Sicht, dass Vorbeugemaßnahmen nicht lohnten, weil sie zu teuer seien, sieht er im Wandel, weil immer mehr Unternehmen von amtlichen und öffentlichen Ermittlungsmaßnahmen betroffen seien. Ein deutlicher Fingerzeig auf die zunehmende Anzahl vor allem von Straf- und Kartellverfahren. Er empfiehlt einen Maßnahmen- und Reaktionsplan für den Fall einer solchen Rechtsstreitigkeit und stellt die Anforderungen an die „E–Discovery-Fähigkeit von Unternehmen" dar. Wichtig sei als erster Schritt, eine Richtlinie zur Dokumentenaufbewahrung zu schaffen (S. 75).

Banackschik widmet sich den Anforderungen der U.S. Discovery und formuliert einen „Leitfaden für Unternehmensjuristen zur Reaktion auf Anforderungen der U.S. Discovery aus der amerikanischen Perspektive" (S. 81-92). Die Autorin zeichnet die Anforderungen an die Discovery in den USA samt der Historie der Discovery nach. Die Anforderungen seien in der Rechtsverordnung für Discovery in den Rules 26–37 niedergelegt. Der Umfang der zugänglichen Informationen sei in Rule 26 (b) 1 niedergelegt: Alles, was relevant ist, steht der anderen Partei auf Anforderung zur Verfügung, solange es sich nicht um bevorrechtigte oder anderweitig geschützte Informationen handelt (S. 86). Wichtig ist, dass die Pflicht zur Aufbewahrung schon in dem Moment einsetzt, wenn mit einem Rechtsstreit vernünftigerweise zu rechnen ist. Die Akten müssten mit einem Vermerk der Pflicht zur Datensicherung versehen werden („Litigation hold").

Mit dem Beitrag von *Wilkse* „E–Discovery im kontinentaleuropäischen Rechtsraum: Discovery–Verfahren in der Schiedsgerichtsbarkeit" (S. 93–105) endet das Kapitel I *Wilske* nimmt eine Prüfung von Regelungen diverser Schiedsgerichtsordnungen vor und kommt zu dem Ergebnis, dass E–Discovery auch in der Schiedsgerichtsbarkeit angekommen ist. Hieraus ergäben sich Gestaltungsmöglichkeiten; eine „Flucht" vor der E–Discovery hält der Autor auch in der Schiedsgerichtsbarkeit nicht für möglich (S. 105).

Zulässigkeit des Datentransfers nach deutschem Recht

Das Kapitel II beginnt mit einem Beitrag von *Laue* zum Thema „E–Discovery und Prüfschema zum internationalen Datentransfer." Plastisch, namentlich anhand eines Beispielfalls, werden die Anforderungen des E–Discovery–Verfahrens anhand des deutschen Datenschutzrechts geprüft. *Laue* kommt zu dem Ergebnis, die Übermittlung von personenbezogenen Daten sei unter den Voraussetzungen des § 28 Abs. 2 Nr. 2a BDSG zulässig, weil die mit der Übermittlung verbundene Zweckänderung dem berechtigten Interesse des Anfragenden entspreche, wenngleich vorab eine datensparsame Datenfilterung sowie – nach Möglichkeit – eine Anonymisierung der Daten durchgeführt werden müsse (S. 115). Er gibt jedoch zu bedenken, dass bei einer Übermittlung von Daten in die USA eine Datenübermittlung in ein Land erfolgt, in dem aus europäischer Sicht kein angemessenes Datenschutzniveau existiert, weswegen das Verbot des § 4 Abs. 2 S. 2 BDSG eingreift. Gleichwohl bejaht *Laue* das Vorliegen des Ausnahmetatbestands § 4c Abs. 1 Nr. 4 BDSG.

Der Betriebsrat

Das Thema von *Meyer* lautet „Deutsches Datenschutzrecht und Betriebsbeteiligung bei E–Discovery in den USA" (S. 123-149). Er legt zunächst den Konflikt zwischen E–Discovery und Datenschutz dar, der bereits bei *Rosenthal* und *Zeunert* angeklungen war. Allerdings führt *Meyer* aus, welche Sanktionen ein fahrlässiger oder vorsätzlicher Verstoß gegen die Aufbewahrungspflichten nach sich ziehen kann. Dies sind u.a. Auferlegung von Gerichts- und Anwaltskosten, Abweisung der Klage im Ganzen oder in Teilen, Verurteilung des Beklagten allein auf Grundlage des klägerischen Vorbringens, Festsetzung von Ordnungsmitteln wegen Missachtung des Gerichts und Festsetzung von Geld und Haftstrafen (S. 127). Er nimmt dann Bezug auf die Rolle des Betriebsrats, dessen Aufgabe die Einhaltung Rechte der Arbeitnehmer ist. Ein echtes Mitbestimmungsrecht bestünde nach § 88 Abs. 1 Nr. 6 BetrVG beim Einsatz technischer Einrichtung zur Überwachung des Arbeitnehmers. In der Folge zeigt er auf, wie sich der Konflikt auflösen lässt (S. 131 ff.). Wenn bei einem E–Discovery–Verfahren Leistungs- und Verhaltensdaten von Arbeitnehmern offengelegt würden, müsse der Betriebsrat eingeschaltet werden. Dieser könne sogar initiativ tätig werden und beim Scheitern der Gespräche die Einigungsstelle anrufen (S. 137). *Meyer* weist darauf hin, dass bei der Offenlegung von Unterlagen in den USA das deutsche Datenschutzrecht nicht gilt. Gleichwohl sei eine Berufung hierauf nicht aussichtslos – die Rechtsprechung des Obersten Bundesgerichts schreibe in diesem Fall eine angemessene Rücksichtnahme auf die besondere Situation ausländischer Prozessparteien vor, was zu einer Interessenabwägung führe. Daneben bestünde die Möglichkeit, sich punktuell von der Offenlegungspflicht zu befreien. Dies beträfe z.B. In-

formationen zwischen Anwalt und Mandant oder Geschäftsgeheimnisse (S. 142 ff.). *Meyer* plädiert am Ende seiner Ausführungen für vorbeugende Maßnahmen. Dazu gehört u.a., nicht mehr benötigte Daten zu löschen.

Brunsch, „Safe in Germany. E–Discovery–Datenschautz im IT Outsourcing" (S. 152 – 170) merkt an, dass immer mehr Kommunikationstechniken mit Cloudtechniken realisiert werden und es zur Auslagerung von Archivierungspflichten kommt. Das Outsourcing sei auch deswegen in Mode, weil Personalkosten eingespart werden. Grundlage für das Outsourcing sei § 11 BDSG, der die sog. Auftragsdatenverarbeitung regelt. *Brunsch* bietet hierfür praktische Hilfestellungen und stellt den 10–Punkte–Katalog des § 11 BDSG vor.

„E-Discovery-Konformität"

Das Kapitel III wird eingeleitet von *Schmid*: „E–Discovery im Kontext IT–Management und Enterprise Data Management" (S. 173 - 204). Er legt die Kernaussagen bezüglich der IT im US- Amerikanischen Zivilprozessrecht dar und fasst sie zusammen: Das beklagte Unternehmen sei gezwungen, grundsätzlich jede Art von Information, auf digitalen Medien gespeichert oder in Papierform, tagesaktuell oder weit in der Vergangenheit zurückliegend, an Unternehmensstandorten in den USA oder zugehörigen Unternehmensstandorten außerhalb der USA gespeichert, an die klagende Partei zu übergeben (S. 175). Diese Datensuche werde in globalen Unternehmen noch schwieriger, weil die Datenmengen ständig wachsen würden. Man würde mehr Daten finden, aber weniger Treffer produzieren. Problematisch sei zudem, dass es alte Dateien gäbe, die über Applikationen erzeugt wurden, die man heute nicht mehr ohne weiteres lesen könne (S. 185). Für die E–Discovery Konformität empfiehlt auch er eine Richtlinie. Dabei sei in Rechnung zu stellen, dass die Daten im Unternehmen einer ständigen Veränderung unterliegen. Als Lösungsansätze sieht er u.a. einheitliche Vorgaben zur Nutzung und „Feuerwehrübungen". Die Einbeziehung externer E–Discovery Beratung lehnt *Schmid* nicht ab, aber sieht es als Zeichen, dass das Kind schon in den Brunnen gefallen sei (S. 194 ff.). Aus der betriebswirtschaftlichen Betrachtung heraus sei die E–Discovery Konformität in jedem Fall dazu geeignet, Geldstrafen und einen Imageverlust zu vermeiden.

Paknad, Jung und *Hampp-Bahnmüller* widmen sich dem Thema „Information Governance als Erfolgsfaktor für Electronic Discovery" (S. 205-230). Sie führen zunächst aus, dass die stark wachsenden Datenmengen und die Anzahl von Regeln ein Problem seien – es werde wichtiger, alle Daten zu löschen, die nicht Bestandteil gesetzlicher oder regulatorischer Anforderungen sind (S. 206). Vorgestellt werden Modelle zum Nutzen der Information Governance (S. 211). Benannt werden Schlüsselanforderungen für die Infrastruktur zur Unterstützung von E–Discovery. Hierzu zählt er den Umgang mit sehr großen Datenmengen, mit langen Aufbewahrungsfristen der Daten, mit einer Vielzahl von Dokumententypen und die Unterstützung der Legal Holds (S. 222).

Wachsende Datenmengen als Herausforderung

Hartmann und *Vernhofen,* „Strategisches Innovations- und Technologiemanagement für E–Discovery" (S. 231 – 246), betonen, dass die Anforderungen an eine E–Discovery sich aus der Neufassung des amerikanischen Zivilprozessrechts (Federeal Rules of Civil Procedure) von 2006 ergeben. Sie definieren E–Discovery als eine computergestützte Methode zur Identifizierung von relevanten Informationen aus einer Vielzahl von elektronischen und Papierdokumenten; es diene der Recherche von Sachverhalten bei internen Prüfungen sowie juristischen Auseinandersetzungen (S. 232). Berichtet wird von der Entwicklung der IKB Data GmbH, die als Shared Service Center der IKB Deutsche Industriebank einen „klassischen" IT Service anbietet und die sich zwischen 2009 und 2011 eine E–Discovery–Infrastruktur aufgebaut hat. Die Autoren skizzieren fünf wesentliche Strukturelemente der E–Discovery, die für die Kompetenzen eines IT–Dienstleiters in diesem Bereich relevant sind (S. 238 ff). Erforderlich ist immer der Einsatz einer Spezialsoftware zur Datenaufbereitung und Datenanalyse. *Hartmann* und *Vernhofen* setzen iConect ein. Diese habe den Vorteil, dass sie webbasiert arbeitet und eine standortunabhängige Analyse ermöglicht.

Datenaufbereitung mit Spezialsoftware

Kiemes und *Pauseback* schließen das Kapitel mit dem Thema „Prozess der E–Discovery in der technischen Umsetzung" (S. 247 - 268). Information Management beginne mit der Schaffung einer zentralen Datenbank nach forensischen Regeln und ende bei der Verfügbarkeit der Information (S. 249). Bei der IKB hätten bei forensischen Untersuchungen die Emails im Fokus gestanden. Welche Informationen benötigt würden, hänge auch von der Ausgangslage in der E–Discovery ab, namentlich ob ein aktiver Klagefall, ein Verteidigungsfall oder eine interne Untersuchung vorliege (S. 252). Auch diese Autoren weisen darauf hin, dass ein

Tool zur Auswertung unumgänglich sei. Anders als bei *Hartmann* und *Vernhofen* wird nicht auf ein spezielles Tool verwiesen, sondern allgemein dargelegt, welche Anforderungen das Tool erfüllen muss. Dazu gehört die Fähigkeit, mit verschiedenen Dokumententypen umgehen zu können, die Einführung von De-Duplizierungswerkzeugen zur Minimierung der Dokumente (Vermeidung von Doppeldateien, insbesondere bei Emails) und zeitliche Filtermöglichkeiten (S. 253). Im Folgenden wird der technische Verlauf einer E–Discovery beschrieben samt der dazu erforderlichen Tools.

In Kapitel IV sind zwei Beiträge enthalten, die sich mit der sog. „The Sedona Conference" (Kurz: TSC) befassen (S. 271 -282). *Bramann* und *Withers* stellen das Prinzip der TSC dar. Diese ist ein in der Stadt Sedona gegründetes Bildungszentrum für Juristen, Anwälte und Wissenschaftler. Teil der Fortbildungsphilosophie ist – anstatt des frontalen Fachunterrichts – eine niedrige Teilnehmerzahl und vor allem fruchtbare Dialoge (S. 273). 2002 wurden die Themen aufwendige Gerichtsverfahren sowie das Management, die Veröffentlichung und die Produktion elektronischer Informationen in Zivilrechtsverfahren als Zukunftsthemen identifiziert. Hierzu wurden Arbeitsgruppen einberufen, die Konzeptpapiere erarbeiten sollten. Im Folgejahr entstand ein Dokument mit dem Namen „The Sedona Principles", das 14 Prinzipien bezüglich der Aufbewahrung, Veröffentlichung und Produktion von elektronischen Informationen im Zivilrecht enthält. Das Dokument ist seit 2003 laut den Autoren in fast 50 Staats- und Bundesgerichten in den USA, Kanada und England zitiert worden.

Daley, Esteban und *Withers* stellen die Ergebnisse von „The Sedona Conference Working Group International Electronic Information Management, Discovery and Disclosure (WG6)" vor (S. 283-306). Hier handelte es sich um eine separate Arbeitsgruppe, die Spannungen zwischen dem US–amerikanischen Verfahren des E–Discovery und den weltweiten Datenschutzrichtlinien hervorhob. Ziel war es nach *Daley, Esteban* und *Withers*, einen vereinfachten Dialog zu ermöglichen und Unterstützung bei der Entwicklung eines Rahmenwerks und von Prinzipien zur Harmonisierung der grenzübergreifenden Offenlegung elektronisch gespeicherter Informationen mit geltenden Datenschutzrichtlinien zu bieten. Das Ergebnis der Arbeitsgruppe ist die bei Drucklegung des Buches im Januar 2011 noch nicht fertiggestellte Schrift „The Sedona Conference International Principles on Data Protection Laws in U.S. Litigation", die im Dezember 2011 veröffentlich wurde.

IV. Zusammenfassung

Das Buch ist eine äußerst gut gelungene Zusammenstellung von Beiträgen rund um das Thema „ E–Discovery" im internationalen Kontext und die Frage, wie Unternehmen auf die damit verbundenen rechtlichen Problemstellungen reagieren sollten. Nahezu jeder der Beiträge zeigt praktische Lösungsmöglichkeiten auf. Der interdisziplinäre Ansatz entspricht der Thematik, wobei die Autoren darauf achten, ihre fachliche Perspektive für jeden der anderen Fachbereiche verständlich zu halten. Das Buch enthält Leitlinien nicht nur zum Schutz in E–Discovery–Verfahren, sondern auch zum Schutz von Unternehmen und der Unternehmens–IT in öffentlichen Ermittlungsverfahren. Wer als rechtlicher Berater ein Unternehmen auf ein Strafverfahren vorbereiten will, wird an dem Thema „Information Governance" wohl kaum vorbeikommen. Mit diesem Buch ist er hierfür bestens gerüstet.