

Valery Bamberger

eDiscovery

Einführung in eDiscovery und dessen Relevanz für Unternehmen

Die Menge an Daten, die Unternehmen generieren und speichern, wächst täglich. Insbesondere bei internen Untersuchungen sowie Rechtsfällen spielen (digitale) Daten eine zentrale Rolle. Unternehmen wie etwa Konzerne oder Anwaltskanzleien wenden sich immer mehr an sogenannte eDiscovery-Experten, um die relevanten Daten zu sammeln, zu bestimmen und zu analysieren. Die vorliegende Arbeit beschäftigt sich mit eDiscovery, dessen Ursprung und heutigen Bedeutung für die Datenbearbeitung und Auswertung. Zusätzlich werden anhand des «Electronic Discovery Reference Model» (EDRM) die technologiegestützten Vorgehensweisen von eDiscovery im Detail betrachtet und erforscht, wobei einzelne eDiscovery Softwarelösungen diskutiert und deren Vorteile für eDiscovery-Spezialisten, Juristen und Anwälte beleuchtet werden. Die Arbeit veranschaulicht des Weiteren Herausforderungen für eDiscovery-Prozesse in der Schweiz.

Beitragsart: Next Generation
Region: Schweiz
Rechtsgebiete: LegalTech; E-Discovery

Zitiervorschlag: Valery Bamberger, eDiscovery, in: Jusletter IT 30. September 2021

Inhaltsübersicht

1. Einleitung
2. eDiscovery – Begriffsdefinition
3. Ursprung
4. Ausgangslage
5. Klassische Vorgehensweise – Electronic Discovery Reference Model
 - 5.1. Information Governance
 - 5.2. Identification
 - 5.3. Preservation
 - 5.4. Collection
 - 5.5. Processing
 - 5.6. Review
 - 5.7. Analysis
 - 5.8. Production
 - 5.9. Presentation
6. Fazit

1. Einleitung

[1] Gemäss SUSSKIND¹ verändern technologische Entwicklungen wie eDiscovery die Art und Weise, wie Rechtsdienstleistungen vollzogen werden. Die Relevanz von eDiscovery ist auf die fortschreitende Digitalisierung zurückzuführen.² Die International Data Corporation (IDC)³ prognostiziert in der im November 2018 publizierte Studie «The Digitization of the World», dass die globale Datasphäre bis im Jahr 2025 auf 175 Zettabytes wachsen wird. Während ein Grossteil dieser Daten normalerweise nicht im Fokus von eDiscovery steht, verdeutlicht der Umfang und das permanente Wachstum an elektronischen Daten die Herausforderungen, mit welchen Unternehmen heutzutage und auch zukünftig konfrontiert sein werden.

[2] Die kontinuierlich steigende Menge an Daten führt dazu, dass die fachübergreifende Zusammenarbeit von Technologie und Recht unerlässlich geworden ist. Bspw. bei kartellrechtlichen Untersuchungen müssen hunderttausende von Dokumenten überprüft werden, daher macht es nach MARTINIS⁴ Sinn, eDiscovery Softwarelösungen einzusetzen, um die zu untersuchende Datenmenge anhand technischer Möglichkeiten zu reduzieren.

2. eDiscovery – Begriffsdefinition

[3] Die OSTERMAN RESEARCH⁵ bezeichnet Discovery als der Prozess des Identifizierens, Bewahrens, Sammelns, Überprüfens, Analysierens und Erstellen von Informationen für zivilrechtliche Fälle. Discovery umfasst somit das Beweiserhebungsverfahren und dient der frühzeitigen Sachverhaltsermittlung sowie der umfassenden Sammlung von Beweismitteln, die für ein Untersuchungsverfahren relevant sein können. Ediscovery kommt bei der Sammlung, Sichtung und Aufbereitung

¹ SUSSKIND, S. 45.

² Vgl. LAWTON, STACEY, DODD, S. 1.

³ GANTZ, REINSEL, RYDNING, S. 3.

⁴ MARTINIS, S. 30.

⁵ Osterman Research, S. 1.

grosser Datenmengen für interne Untersuchungen oder Gerichtsverfahren zum Einsatz und umfasst alle elektronisch gespeicherten Informationen wie E-Mails, Sofortnachrichten und andere elektronische Inhalte, die auf Desktops, Laptops, Dateiservern, Smartphones, Heimcomputern oder vielen anderen digitalisierten Plattformen gespeichert werden können.⁶

3. Ursprung

[4] eDiscovery hat seine Wurzeln in den USA, als das US Supreme Court im Dezember 2006 die Federal Rules of Civil Procedure (FRCP) änderte.⁷ Die FRCP geben den prozessrechtlichen Rahmen für Zivilverfahren vor den Bezirksgerichten der Vereinigten Staaten vor. Ihr Zweck ist es, «die gerechte, schnelle und kostengünstige Bestimmung jeder Handlung und jedes Verfahrens sicherzustellen».⁸ Die erneuten Änderungen im Jahr 2006 haben die heutige Funktionsweise von eDiscovery wesentlich geprägt. Mit dieser Revision wurden die Voraussetzungen für die Beweissicherung, sowie für die Datenaufbereitung und anschliessende Datenüberlieferung an Dritte definiert. Eine der signifikantesten Änderungen bestand darin, dass elektronisch gespeicherte Daten, «Electronically Stored Information» (ESI), neu zu den legitimen Beweismitteln einer Untersuchung gezählt werden und ESI als gesetzlich bestimmten Begriff definiert wurde.⁹

4. Ausgangslage

[5] Die Schweiz ist mittlerweile auch vom eDiscovery-Verfahren betroffen. ROSENTHAL¹⁰ schildert vier Szenarien, in denen Schweizer Unternehmen eDiscovery anwenden könnten. Zum einen könnte eDiscovery bei Zivilprozessen, in welchen schweizerische Unternehmen in den Vereinigten Staaten oder in Ländern, mit ähnlichen Verfahrensregeln, angeklagt werden, an Bedeutung gewinnen.¹¹ Auch bei internen Untersuchungen, wegen möglichem Fehlverhalten oder Compliance-Verstössen¹² werden eDiscovery-Spezialisten kontaktiert, um Nachforschungen zu veranlassen. Ausserdem können schweizerische oder ausländische Behörden jederzeit interne Unternehmensdokumente einfordern, wenn Verdacht auf Rechtswidrigkeit oder schuldhaftes Rechtsverletzung besteht. Art. 158 ZPO¹³ erläutert die vorsorgliche Beweisführung, dem zufolge dürfen Beweise nicht nur in dringlichen Fällen, sondern auch schon vor oder während eines Prozesses verlangt werden können. Auch bei datenschutzrechtlichen Auskunftsbegehren wird eDiscovery verwendet.¹⁴ Schweizer Unternehmen mit Tochtergesellschaften in den USA sind ver-

⁶ Vgl. Osterman Research, S. 2.

⁷ DRÄYER-DE MOOR, ZEUNERT.

⁸ United States Courts <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure> (07.12.20).

⁹ Vgl. VINJUMUR, S. 1.

¹⁰ ROSENTHAL, FOLIE S. 2.

¹¹ Vgl. ROSENTHAL, S. 2.

¹² DRÄYER-DE MOOR, TEO, SWISS FTS.

¹³ Vgl. Art. 158 ZPO <https://www.admin.ch/opc/de/classified-compilation/20061121/202007010000/272.pdf> (Stand: 08.12.20).

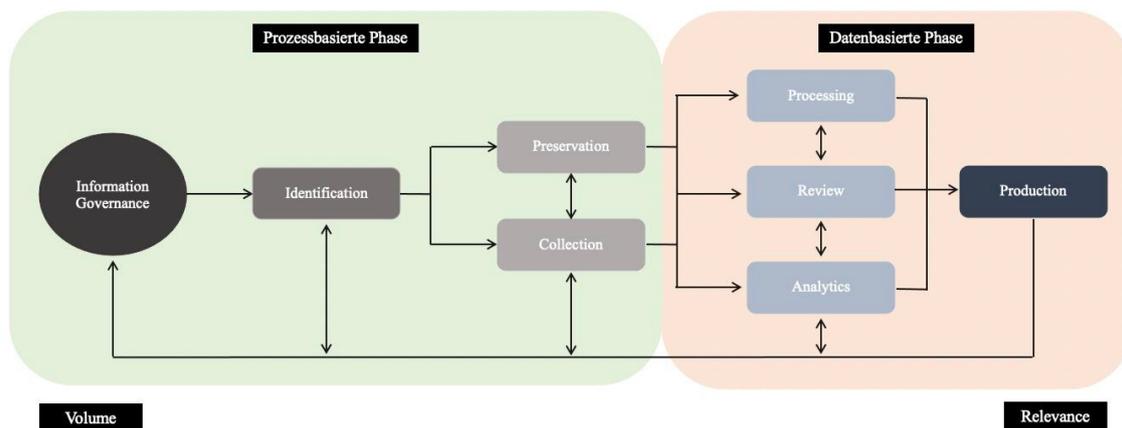
¹⁴ ROSENTHAL, FOLIE 2.

pflichtet, auf Anfrage der amerikanischen Behörden bestimmte Daten herauszugeben.¹⁵ Diese Ausgangslagen führen dazu, dass eDiscovery eine wesentliche Bedeutung im Schweizer Rechtsmarkt gewinnt.

5. Klassische Vorgehensweise – Electronic Discovery Reference Model

[6] Der eDiscovery Standardprozess basiert auf dem EDRM (Electronic Discovery Reference Model)¹⁶. Das EDRM wurde 2005 von den Discovery-Experten George Socha und Tom Gelbmann entwickelt,¹⁷ um eine einheitliche Vorgehensweise für eDiscovery zu definieren. In der nachfolgenden Abbildung sind die neun eDiscovery-Stufen dargestellt. Die Aktivitäten des Modells lassen sich in zwei Phasen einteilen. Die erste Phase umfasst den Prozess der Verwaltung, Bewahrung und Sammlung der Informationen. In der zweiten Phase wird ein stärkerer Fokus auf die einzelnen Daten gelegt, welche verarbeitet, überprüft, analysiert, produziert und schliesslich an Dritte präsentiert werden.¹⁸

Abbildung 1: Electronic Discovery Reference Model



Anmerkung: Eigene Darstellung in Anlehnung an EDRM.¹⁹

5.1. Information Governance

[7] Informationen sind sehr wertvoll, aber können auch ebenso ein grosses Risiko darstellen; aus diesem Grund hat «The Sedona Conference»²⁰ die Informationsführung als die Grundlage von eDiscovery-Prozessen definiert. Die Information Governance kümmert sich um die Richtlinien,

¹⁵ Vgl. FAVALLI, Digital Law Bites #26.

¹⁶ <https://edrm.net/edrm-model/> (Stand: 08.12.20).

¹⁷ <https://www.logikcull.com/guide/introduction-to-ediscovery-basics> (Stand: 08.12.2020).

¹⁸ Vgl. <https://www.exterro.com/basics-of-e-discovery/e-discovery-process> (Stand: 08.12.20).

¹⁹ <https://edrm.net/edrm-model/> (Stand: 08.12.20).

²⁰ Vgl. The sedona conference, S. 104.

Verfahren und Verwaltung der Informationen, um Risiken und Kosten, die beim eDiscovery-Verfahren aufkommen, zu mindern.²¹

5.2. Identification

[8] Zur Datenidentifizierung kommt es, wenn ein Rechtsstreit vorhersehbar wird und Parteien gesetzlich verpflichtet sind, die relevanten ESI zu verlangen und zu erhalten. Um diesen Schritt durchführen zu können, müssen Schlüsselpersonen der Untersuchung sowie auch Datenquellen (Server, PC, Laptop, Mobiltelefone etc.) identifiziert werden. Die Wichtigkeit hier besteht darin, sich mit dem potenziellen Umfang und den technischen Fragen des vorliegenden Prozesses auseinander zu setzen.²²

5.3. Preservation

[9] Parteien müssen sicherstellen, dass die für das Verfahren relevante ESI aufbewahrt und nicht verändert oder zerstört werden.²³ Da ESI aufgrund des Datenschutzes nach einer gewissen Dauer gelöscht werden, ist hier besondere Vorsicht geboten, da das vorsätzliche Löschen relevanter Daten strafbar sein kann.²⁴ Um Daten vor Verlust und Veränderung zu schützen muss, bereits früh ein «Litigation Hold»²⁵ ausgesprochen werden.²⁶

5.4. Collection

[10] Die Datenbeschaffung von ESI stellt eine grosse Herausforderung dar, da die Daten forensisch sichergestellt werden müssen. Es sollte eine anerkannte und geprüfte Methode angewendet werden, um sicherzustellen, dass die Inhalte und Metadaten, wie zum Beispiel Erstellungsdatum und Dateigrösse, durch den Erhebungsprozess nicht verändert werden.²⁷ Aus diesem Grund werden die Datenbeschaffungen in der Regel von IT und eDiscovery-Spezialisten vorgenommen.²⁸

5.5. Processing

[11] Die Datenverarbeitung umfasst die Vor- und Aufarbeitung der gesammelten ESI für die spätere Analyse und Überprüfung. Für diese Phase werden aufgrund der grossen Datenmengen i.d.R. Datenverarbeitungssoftwares gemietet.²⁹ Mit diesen Softwares wie bspw. Nuix³⁰ werden sowohl

²¹ Vgl. <https://www.logikcull.com/guide/introduction-to-ediscovery-basics> (Stand: 08.12.20).

²² Vgl. Osterman Research, S. 10.

²³ Vgl. <https://www.logikcull.com/guide/introduction-to-ediscovery-basics> (Stand: 08.12.20).

²⁴ Vgl. DRÄYER-DE MOOR, ZEUNERT.

²⁵ Auch Legal Hold genannt, ist eine rechtliche Auflage, die die Datensicherung für juristische Zwecke bedeutet.

²⁶ ROSENTHAL, S. 5.

²⁷ <https://www.exterro.com/basics-of-e-discovery/e-discovery-process> (Stand: 08.12.20).

²⁸ DRÄYER-DE MOOR, TEO, SWISS FTS.

²⁹ ROSENTHAL, FOLIE 5.

³⁰ <https://www.nuix.com/> (Stand: 12.12.20).

die beschaffene unstrukturierten (wie Emails und andere lose Dateien) als auch die strukturierten Dateien aus ihren Ordnern extrahiert und irrelevante Systemdaten gelöscht (DeNisting)³¹. Anschliessend werden die Daten in ein lesbares Format übertragen.³² Nuix hat zum Ziel, den Datenumfang für die nachfolgende Überprüfung zu reduzieren, dieser Vorgang wird auch Culling³³ genannt. Dabei werden unnötige Systemdaten gelöscht und das Datenmass anhand der Duplizierungen verringert.³⁴ Eine weitere Massnahme, welche ein Teil des Culling darstellt, ist das Definieren von relevanten Suchbegriffe, die für die Untersuchung von Bedeutung sein können. Auf diese Weise wird der Untersuchungsumfang reduziert und die Anzahl potenziell relevanter Dateien maximiert.³⁵

5.6. Review

[12] In der Überprüfung werden die Dokumente, die in die Reviewsoftwares, wie etwa Relativity³⁶ exportiert wurden, überprüft und als relevant oder irrelevant für den Rechtsfall klassifiziert. Diese Überprüfung übernehmen meist Anwaltskanzleien. Aufgrund der enormen Datenmenge kann die detaillierte manuelle Datensichtung viel Zeit in Anspruch nehmen und ist daher schwierig zu bewerkstelligen. Aus diesem Grund wurde TAR (Technology-Assisted Review) bei eDiscovery-Prozesse eingeführt. Es handelt sich dabei um eine technologiegestützte Überprüfung, einer prädiktiven Kodierungstechnik, die mit künstlicher Intelligenz (KI) den Prozess der Dokumentenprüfung beschleunigt.³⁷

[13] Dass die manuelle Überprüfung im Vergleich zur technisch automatisierten Methode ineffizienter ist, haben auch einige Studien bereits in den ersten Jahren der eDiscovery Entwicklung gezeigt. Im Jahr 2009 haben die zwei eDiscovery-Experten GROSSMAN und CORMACK im jährlichen Forschungsprojekt der TREC Legal Track Organisation Daten zur prädiktiven versus menschlichen Überprüfung analysiert, und kamen dabei zum Schluss, dass prädiktive Kodierung nicht nur effizienter ist, sondern auch viel kostengünstiger.³⁸ Der Einsatz prädiktiver Kodierungstechniken führe fast zu einer fünfzigfachen Kostenersparnis.³⁹ Der Computeralgorithmus, wie etwa bei der Software Brainspace⁴⁰, kann durch das Lesen der Dokumente nach relevanten Wörtern suchen und sie anhand ihres Inhaltes in Gruppen einteilen (Conceptual Clustering).⁴¹ Brainspace sowie die meisten anderen gängigen eDiscovery Tools stellen die Daten visuell dar, um ein schnelleres Verständnis der Daten zu erlangen.⁴² Dabei werden ähnliche Dokumente gruppiert

³¹ Vgl. <https://www.exterro.com/basics-of-e-discovery/e-discovery-process> (Stand: 08.12.20).

³² Vgl. DRÄYER-DE MOOR, ZEUNERT.

³³ Vgl. SONDHI, ARORA, S. 290.

³⁴ Vgl. DRÄYER-DE MOOR, ZEUNERT.

³⁵ Vgl. DRÄYER-DE MOOR, ZEUNERT.

³⁶ <https://www.relativity.com/> (Stand: 12.12.2020).

³⁷ Vgl. VINJUMUR, S. 3.

³⁸ GROSSMAN, CORMACK, S. 2.

³⁹ GROSSMAN, CORMACK, RN 52.

⁴⁰ <https://www.brainspace.com/> (Stand: 15.12.20).

⁴¹ Vgl. DILLEN, HULSBOS.

⁴² Vgl. ROSENTHAL, S. 10.

und erleichtern es dem Ermittler, einen Überblick zu gewinnen. So wird unter anderem ersichtlich, wo noch weiterer Untersuchungsbedarf herrscht.⁴³

[14] Trotz den vielen Vorteilen, die KI bietet, werden menschliche Reviewers für Untersuchungen weiterhin gebraucht. Laut HULSBOS⁴⁴ muss es eine Interaktion zwischen dem Algorithmus und dem Untersucher geben. Bei der Assisted Review werden eine Reihe von relevanten und nicht relevanten, von menschlichen Reviewer vorbeschrifteten Beispielen dem Algorithmus zur Verfügung gestellt. Mit diesen Dokumenten wird er dann trainiert, um zu erkennen, ob ein Dokument relevant oder nicht relevant ist, auch Überwachtes maschinelles Lernen genannt. So kann er weitere Dokumente markieren und ihnen eine Relevanzbewertung zwischen 1 und 100 geben. DILLEN erklärt anhand eines Fallbeispiels, dass die Dokumente, mit einer hohen Bewertung und zuvor als nicht relevant gekennzeichnet waren, in einer weiteren Sichtsphase überprüft wurden und manchmal ihre Kodierung änderten. Mit dem konnte das Risiko, relevante Dokumente zu übersehen, reduziert werden.⁴⁵

5.7. Analysis

[15] In der Analyse liegt der Fokus insbesondere auf dem Inhalt und dem Kontext. In dieser Phase werden der Untersuchungsgegenstand sowie die Schlüsselpersonen i.d.R. durch zuständigen Anwälte identifiziert.⁴⁶

5.8. Production

[16] Datenherausgabe bedeutet, dass die als rechtsfallrelevante ESI den Behörden zwecks Beweisaufnahme übergeben werden. Für die Erstellung dieser Dokumente werden Formatregeln vorgegeben und festgelegt. Grundlegend zu beachten sind dabei die Formatbedingungen für die technische Dokumente Anfertigung. Die Dokumente können als Natives (Originalkopie) oder als Images in PDF oder TIFF Format ausgehändigt werden. Zusätzlich werden Redactions (Zensuren) erstellt, die wegen des Anwalts-Privilegs oder der Vertraulichkeit eingefügt werden müssen.⁴⁷

[17] Strengstens bei dieser Phase zu berücksichtigen ist das Verbot von Handlungen für fremde Staaten in der Schweiz (Art. 271)⁴⁸. Der Artikel im schweizerischen Strafgesetzbuch (StGB)⁴⁹ ist auch mit dem Begriff «Swiss Blocking Statue» bekannt und erläutert, dass das Handeln für fremde Staaten ohne Bewilligung in der Schweiz verboten ist. Somit ist die Beweiserhebung für ausländische Gerichts- oder Aufsichtsverfahren und die Überlieferung von Informationen, die Schweizer Unternehmen gehören, an ausländische Behörde beschränkt oder sogar ganz blockiert.⁵⁰

⁴³ Vgl. DILLEN, HULSBOS.

⁴⁴ HULSBOS.

⁴⁵ DILLEN.

⁴⁶ Vgl. <https://www.logikcull.com/guide/introduction-to-ediscovery-basics> (Stand: 08.12.2020).

⁴⁷ Vgl. DRÄYER-DE MOOR, TEO, Swiss Fts.

⁴⁸ GOGNIAT, Rz 1.

⁴⁹ <https://www.admin.ch/opc/de/classified-compilation/19370083/index.html> (Stand: 16.12.20).

⁵⁰ Vgl. OETIKER.

[18] Das Datenschutzgesetz stellt eine weitere Hürde bei der Übermittlung dar. Nach amerikanischem Recht haben die Parteien die Rechtspflicht, alle Dokumente, die für den Rechtsstreit relevant sein könnten, vorzulegen. Diese umfangreiche Datenherausgabepflicht kann sogar im Vorfeld eines Zivilprozesses stattfinden. Der schweizerische Datenschutz schränkt die Übergabe der Daten jedoch massiv ein.⁵¹ «Das Schweizer Datenschutzgesetz ist geprägt von Grundgesetzen, die zu einem Konflikt zwischen dem eDiscovery Mechanismus mit zahlreichen diesen Grundsätzen führt», laut MATHYS.⁵²

[19] Der Grundsatz der Rechtmässigkeit (Art.4 Abs. 1 DSG)⁵³ erläutert, dass Personendaten nur rechtmässig bearbeitet werden dürfen. Ein weiterer Grundsatz ist die Zweckbindung und Transparenz (Art. 4 Abs. 3 und 4. DSG)⁵⁴, Personendaten dürfen nur zum Zweck bearbeitet werden, welcher bei der Beschaffung angegeben wurde. Zudem muss der Zweck der Daten für die betroffenen Personen erkennbar sein. Es gilt auch der Grundsatz der Verhältnismässigkeit, (Art. 4 Abs. 2 DSG)⁵⁵, da eDiscovery Untersuchungen anfangs meist zu unspezifisch sind, und es ziemlich unklar ist, welche Daten und wie viele davon betroffen sind. Ein weiteres Hindernis stellt Art. 5 DSG⁵⁶, indem die Richtigkeit der Daten erläutert werden. Hier handelt es sich um Datenmodifikationen, welche sich als Beweismanipulationen herausstellen könnten. Art. 6 der DSG⁵⁷ erläutert noch weitere Grundsätze, die sich mit den eventuell fehlenden Schutzrichtlinien bei grenzüberschreitenden Bekanntgaben befassen. Laut Art. 13 DSG⁵⁸ gibt es jedoch Rechtfertigungsgründe, warum Daten herausgegeben werden können. Um eDiscovery Daten trotz des Datenschutzgesetzes zu produzieren, sollen diese mehrfach durchsucht und gefiltert werden, mit dem Ziel, dass der Datenumfang kleiner und somit bestimmter wird.

5.9. Presentation

[20] Bei diesem Schritt werden die produzierten elektronischen Beweismittel bei Anhörungen und Gerichtsverfahren präsentiert.

6. Fazit

[21] Aufgrund der stetig wachsenden Datensphäre und der steigenden Anzahl von Zivilprozessen gewinnt eDiscovery zunehmend an Relevanz. Dank KI und dem maschinellen Lernen kann ein grosser Datenbestand effizient durchsucht werden, wodurch auch erhebliche Kosten gespart werden können. Grenzüberschreitende eDiscovery wirft jedoch rechtliche Fragen auf, insbesondere im Hinblick auf das Datenschutzrecht und dem «Swiss Blocking Statue». Diese Erschwernisse sollten bei eDiscovery Untersuchungen immer klar im Vordergrund stehen, damit keine

⁵¹ Vgl. ROSENTHAL, ZEUNERT S. 24.

⁵² MATHYS, Podcast.

⁵³ Art. 4 Abs. 1 DSG.

⁵⁴ Art. 4 Abs. 3/4 DSG.

⁵⁵ Art. 4 Abs. 2 DSG.

⁵⁶ Art. 5 DSG.

⁵⁷ Art. 6 der DSG.

⁵⁸ Art. 13 DSG.

Rechtsverletzungen beim Überliefern der Daten auftreten können. Zudem werden immer mehr Unternehmen ihre Daten auf einer sogenannten Cloud speichern. Diese Art online Datenspeicher stellt eDiscovery vor neuen Herausforderungen. So lässt sich etwa der physische Standort der auf der Cloud gespeicherten Daten nicht ohne Weiteres bestimmen. Denn im Normalfall weisen auf Cloud gespeicherte Daten mehrere Standorte auf, was auch Fragen über den Inhaber nach sich zieht.⁵⁹

[22] Trotz der ständigen Weiterentwicklung von «ESI» und der Digitalisierung muss eDiscovery zweifellos mithalten können. Unternehmen werden sich zukünftig immer mehr an eDiscovery-Spezialisten wenden mit dem Verlangen, Zeit und Kosten zu sparen. Die erhöhte Nachfrage nach eDiscovery resultiert darin, dass die Arbeitsweise im Rechtsmarkt nachhaltig verändert werden muss.

VALERY BAMBERGER, B.A. Studentin der Rechtswissenschaften an der Universität St.Gallen (HSG).

⁵⁹ SYNDER, S. 44–45.