Die Verfasserin widmet sich dem südafrikanischen Intellectual Property Laws Amendment Act 2013, der im Anhang des Buches vollständig abgedruckt ist. Der Schutz indigenen Wissens steht im Zusammenhang mit der Aufwertung traditioneller Lebensphilosophie, der Erhaltung der Biodiversität, aber auch der finanziellen Beteiligung der indigenen Gemeinschaften an der Verwertung solchen traditionellen Wissens. Es geht um einen wirtschaftlichen Ausgleich, der früher nur vertraglich möglich war, jetzt aber in gesetzlichen Bestimmungen festgelegt ist. Nach einer knappen Einleitung behandelt die Verf. zunächst die Stellung der Entwicklungsländer, insbesondere der Republik Südafrika, im globalen Immaterialgüterrechtssystem und widmet sich dann der Erläuterung der relevanten Begrifflichkeiten, insbesondere der Begriffe «indigen» oder «traditionell». Dann folgt ein Abschnitt über bereits bestehende Regelwerke zum Schutz indigenen Wissens. Der Hauptteil der Arbeit gilt dann dem neuen «Intellectual Property Laws Amendment Act 2013» der Republik Südafrika (S. 73 – 215).

Ausführlich und kenntnisreich wird erfasst, was eine indigene Gemeinschaft in Südafrika darstellt. Es «ist davon auszugehen, dass der südafrikanische Gesetzgeber sämtliche schwarze Gemeinschaften als indigen ansieht, die customary law befolgen» (S. 148). Hinzu tritt das Bewusstsein, einer solchen Gemeinschaft anzugehören, ein Zusammengehörigkeitsgefühl. Man wird an *Mancinis* Begriff der Nation erinnert, der außer den äußeren Elementen noch ein solches Bewusstsein («Coscienza della Nazionalità», *Mancini*, Dellla nazionalità come fondamento del diritto delle genti, 1851, ed. *Jayme*, 2000, S. 45) verlangt. Insgesamt geht es um Miturheberschaft (S. 156).

Die Frankfurter Dissertation, die auf Studien in Südafrika beruht, betritt vielfach Neuland. Sie ist klar und spannend geschrieben, hält auch gelegentlich mit der Kritik nicht zurück. Der Leser lernt viel über die Sonderstellung des neuen südafrikanischen Rechtssystems und seine Originalität, aber auch über den Mut des dortigen Gesetzgebers, solche Fragen zu regeln.

Prof. em. Dr. Dr.h.c. mult. *Erik Jayme*, Heidelberg

Borges, Georg/Meents, Jan Geert (Hg.): Cloud Computing: Rechtshandbuch. C.H. Beck Verlag, München 2016, XXXIII + 734 S., ISBN 978-3-406-64590-7, € 139.–/CHF (fPr) 195.–

Cloud Computing ist aus der modernen Wirtschaft nicht mehr wegzudenken. Die vielfältigen berührten Rechtsfragen unternimmt das zu besprechende Rechtshandbuch umfassend darzustellen. Es richtet sich ausweislich des Ver-

lagsprogramms vorrangig an die beratende Praxis. Als Herausgeber zeichnen Georg Borges (Universität des Saarlandes) und *Jan Geert Meents* (DLA Piper) verantwortlich. Beide sind auf dem Gebiet des Cloud Computing durch Veröffentlichungen hervorragend ausgewiesen. *Borges* leitet zudem die Arbeitsgemeinschaft «Rechtsrahmen des Cloud Computing» des Bundesministeriums für Wirtschaft und Energie; *Meents* ist Mitglied in der «Expert Group on Cloud Computing Contracts» der EU-Kommission. Mit ihrer Verbindung von Praxis und Wissenschaft stehen die Herausgeber stellvertretend für das gesamte Autorenteam.

Das Gesamtwerk ist übersichtlich gegliedert nach Kapiteln und Paragraphen. Neben dem Gesamtinhaltsverzeichnis finden sich auch zum Beginn der einzelnen Abschnitte Verzeichnisse, die das Arbeiten erleichtern. Ob es sich bei den dortigen Literaturhinweisen um weiterführende Leseempfehlungen oder ein Nachweisregister handelt, wird jedoch nicht ganz deutlich. Jedenfalls gehen die unspezifischen Hinweise auf Standardkommentare und -handbücher (bspw. zu BGB, BDSG, UrhG oder TKG) über letzteres nicht hinaus. Ausweislich der zitierten Literatur scheinen sich die meisten Bearbeitungen auf dem Stand Ende 2014 zu befinden; hier bestehen durchaus Unterschiede in den einzelnen Abschnitten.

Das Handbuch beginnt mit einer Darstellung der technischen und betriebswirtschaftlichen Grundlagen (S. 1–37) von *Krcmar*. Diese dient auch einer einheitlichen Begriffsbildung. Das zweite Kapitel bildet einen ersten Schwerpunkt des Handbuchs und behandelt das Vertragsrecht (S. 39–208). Das Internationale Privatrecht (§ 3) übernimmt *Borges*. Er hält eine vertragstypologische Einordnung der Cloud-Computing-Verträge für unnötig, da diese gemäß Art. 4 Rom-I-VO mangels Rechtswahl stets dem Recht des gewöhnlichen Aufenthaltsorts des Cloud-Anbieters unterlägen (Rn. 17), soweit es sich nicht um Verbraucherverträge handelt (für diese gilt Art. 6 Rom-I-VO, eingehend Rn. 20 ff.). Die Darstellung des materiellen Vertragsrechts ist getrennt nach den Beziehungen zwischen Nutzer und Anbieter einerseits (§ 4) und der Anbieter untereinander (§ 5). Den Cloud-Computing-Vertrag sieht *Meents* in Anlehnung an Bundesgerichtshof und im Einklang mit der herrschenden Literatur als typengemischten Langzeitvertrag an (Rn. 45 ff.), der neben den wesentlichen mietvertragsähnlichen Pflichten auch weitere (ggf. dienst- oder werkvertragliche) Leistungspflichten des Cloud-Anbieters enthalten kann (Rn. 57 ff.). An dieser Einordnung orientiert sich dementsprechend die weitere Darstellung der Vertragspflichten und des Rechts der Leistungsstörungen. Der Cloud-Nutzer muss also insbesondere eventuelle Mängel dem Vertragspartner anzeigen, um nicht seiner Gewährleistungsrechte verlustig zu gehen (Rn. 89). Den Cloud-Anbieter-Kooperationsvertrag ordnet *Büchner* als «Typenkombina-

tions-Dauerschuldvertrag mit *sui-generis*-Elementen» ein, weswegen er ein modulares System der miteinander kombinierbaren möglichen Leistungsinhalte nach Art eines Baukastens verwenden möchte (Rn. 16 f.). Die weitere Darstellung der potentiellen Vertragsinhalte erinnert folglich ein wenig an ein Formularbuch.

Zweiter Schwerpunkt ist das dritte Kapitel, das sich dem Datenschutz widmet (S. 209–395). Bearbeitet wurde es großteils von *Borges*. Dieser stellt nach einer Einführung die Möglichkeiten und Grenzen der Auftragsdatenverarbeitung im Stile einer Großkommentierung (§ 7, S. 225–276) dar. Mit den «weiteren Grundlagen» (§ 8, S. 278–301) sind v.a. die datenschutzrechtliche Einwilligung und die Rechtfertigung nach § 28 BDSG gemeint. Daran schließen sich die Bestimmung des anwendbaren Datenschutzrechts bei Auslandsbezug (§ 9, S. 298–355), die technische Datensicherheit von *Sorge* und *Cahsor* sowie der «kommunikationsrechtliche Datenschutz» von *Nolte* (§ 11, S. 380–395) an, also die dem BDSG gemäß § 1 Abs. 3 BDSG vorgehenden Spezialregelungen aus TKG und TMG. Vermissen könnte man allenfalls eine Auseinandersetzung mit den Besonderheiten des arbeitsrechtlichen Datenschutzes.

Das nächste Kapitel ist mit «Haftungsfragen und Compliance» überschrieben. Entgegen dem hier und vom Titel des § 12 («Haftungsaspekte», S. 397–415) erweckten Eindruck sind Haftungsfragen über das Handbuch verstreut. Das folgt schon aus der verfolgten systematischen Ordnung nach Rechtsgebieten. Das Stichwortregister kann jedoch nicht helfen, es kennt nur «Haftungsprivilegierung» und «Haftungsrisiko». Die vertragliche Haftung (des Anbieters) wird schon in §§ 4 und 5 mit erörtert. Dort ist sie den einzelnen Rechtsfragen zugeordnet (z.B. Hauptpflichten, Sekundärpflichten; vertragliche Haftungsbeschränkungen insb. mittels AGB, «faire und angemessene Haftungsverteilung»). In § 12 werden von *Borges* deshalb vor allem die deliktischen Anspruchsgrundlagen und die Auswirkungen des IT-Sicherheitsgesetzes untersucht. Demgegenüber wird die Störerhaftung den «Immaterialgüterrechtlichen Aspekten» (§ 14, S. 441–472) zugeordnet. Dort hat sie wohl auch die größte Bedeutung, wird von *Lehmann* aber auch unter Einbeziehung der privatrechtlichen Anspruchsgrundlagen und der aus dem TMG behandelt. *Behling* hat den Abschnitt zur Compliance (§ 13) übernommen, der sich vor allem an den Compliance Officer richtet. Es handelt sich um einen zusammenfassenden Überblick über die typischen Probleme beim unternehmerischen Cloud Computing; ein Ritt durch das Wirtschaftsrecht.

Im folgenden Kapitel sind sachlich recht disparate Themen zusammengefasst. Es beginnt mit dem Internationalen Zivilverfahrensrecht (§ 15, S. 474–490). Im Fokus stehen die Vorschriften der EuGVVO; das autonom

deutsche Zuständigkeitsrecht wird nur ganz überblicksweise wiedergegeben. *Thole* betont die autonome Begriffsbildung und stellt heraus, dass die vertragstypologische Einordnung im Regelfall unerheblich ist, im Rahmen des Art. 7 Nr. 1 EuGVVO jedoch relevant werden kann (Rn. 14 ff.). Anschauliche Fallbeispiele runden hier die Darstellung ab. Unter dem «Internationalen Zugriff auf Daten» des § 16 (S. 491–511) verbirgt sich – wie der eigentliche Titel im Klammerzusatz anzeigt – ein recht spezieller Abschnitt zur Discovery des US-amerikanischen (Bundes-)Zivilprozesses. Dieses besondere Beweiserhebungsverfahren findet nur auf Streitigkeiten unter Geltung des US-amerikanischen Rechts Anwendung und richtet sich nicht etwa nach dem Standort der Cloud-Server. Handelt es sich um einen solchen Rechtsstreit, sind dann aber sämtliche relevante, also auch «international gelagerte» Unternehmensdaten herauszugeben (Rn. 22). Aus den hoheitlichen Zugriffsmöglichkeiten für deutsche oder US-amerikanische Behörden will *von Diemar* jedoch keine datenschutzrecht Beschränkung für den Einsatz von Cloud Computing in den USA oder anderswo ableiten (§ 17 Rn. 46 ff.). Dopplungen in der Darstellung können auch hier nicht ganz ausgeschlossen werden, wenn die strafprozessualen Zugriffsrechte im späteren § 20 von *Gercke* (S. 581–605) erneut dargestellt werden.

Das letzte Kapitel fasst spezifische Darstellungen zu zwei wichtigen Wirtschaftsbereichen zusammen: der öffentlichen Hand (§§ 22, 23) und dem Finanzwesen (§ 24). § 22 von *Müller-Terpitz* (S. 643–660) zur Nutzung von Cloud-Computing durch die öffentliche Hand in Deutschland ist dabei wohl im Zusammenhang mit den umfangreicheren Ausführungen von *Roth* zum Vergaberecht (§ 18, S. 533–558) zu lesen. § 23 wiederum enthält Länderberichte zum Einsatz und zur wirtschaftspolitischen Förderung von Cloud-Computing durch die Öffentliche Hand im Ausland. Leider wird nicht offengelegt, aufgrund welcher Kriterien hier die Wahl auf die USA, Singapur, das Vereinigte Königreich und Frankreich fiel. *Schindler* kommt jedenfalls zu praktisch relevanten Ergebnissen, wenn er die staatsgeförderten französischen Cloud-Anbieter aus Erwägungen der Datensicherheit als Alternative zu anderen Anbietern betont (Rn. 41).

Insgesamt sind die Darstellungen natürlich sprachlich und inhaltlich auf einem hohen Niveau. Es sind die Wiederholungen einzelner Themenbereiche, die auf den wechselnden Perspektiven der einzelnen Abschnitte beruhen, die als Schwäche des Gesamtwerkes angesehen werden könnten. Gleichwohl wird so erreicht, dass die Bearbeitungen mit wenigen Binnenverweisen auskommen und weitgehend auch allein verständlich sind.

Jun.-Prof. Dr. *Frank Rosenkranz*, Ruhr-Universität Bochum