

Selbstständigkeit angeht, muss der Eigenanteil des neuen Werkes objektiv erkennbar sein. Damit bleibt die Appropriation Art völlig zu Recht auf der Strecke (S. 172; vgl. *Schack*, Kunst und Recht, 2. Aufl. 2009, Rn. 350 ff.). Indizien für die Selbstständigkeit sind eine transformative Werknutzung (die antithematische eingeschlossen) und die fehlende Substitutionskonkurrenz (S. 176 f.).

Zentraler Ort der verfassungskonformen Auslegung ist das Freiheitskriterium in § 24 UrhG (S. 178 ff.). Das wird von *Summerer* im Wesentlichen darauf verkürzt, ob der Originalurheber spürbar beeinträchtigt wird. Damit läuft alles wieder auf die übliche Interessenabwägung hinaus. Hier will *Summerer* pornografische Transformierungen im Rahmen von § 24 an § 14 UrhG scheitern lassen (S. 183, 186 f.). Den starren Melodienschutz in § 24 II UrhG hält sie daneben für nicht mehr notwendig und mit Recht für unhaltbar (S. 185 f.). Verfassungs- oder unionsrechtliche Bedenken gegen eine derartige Auslegung von § 24 UrhG bestehen nicht (S. 188–199); selbst wenn man § 24 UrhG funktional als Schranke verstünde, sei der Dreistufentest gewahrt.

Im siebten Kapitel (S. 200–216) wendet *Summerer* ihre Auslegung von § 24 UrhG auf die verschiedenen, im ersten Kapitel erwähnten Erscheinungsformen von Fan Art an. Im Ergebnis (S. 217–222) kommt *Summerers* Auslegung von § 24 UrhG den Urhebern von Fan Art etwas entgegen, ohne die Grundstrukturen des Urheberrechts über den Haufen zu werfen. Das ist wohltuend und lesenswert.

Prof. Dr. *Haimo Schack*, Kiel

Hilber, Marc (Hg.): Handbuch Cloud Computing. Verlag Dr. Otto Schmidt, Köln 2014, 801 S., ISBN 978-3-504-56091-1, € 119.–/CHF (fPr) 149.–

Kaum ein Begriff elektrisiert die IT-Industrie derzeit so sehr wie die Cloud. Dass die Technik im juristischen Alltag angekommen ist, belegt das Erscheinen gleich mehrerer Handbücher zu diesem Thema. Das von *Hilber* herausgegebene Werk soll Unternehmen eine «umfassende Orientierung geben», die Cloud-Services einkaufen oder anbieten (S. IX). Diesem Anspruch wird das Handbuch gerecht. Ausgewiesene Spezialisten, vorwiegend Rechtsanwälte, führen verständlich und zuverlässig durch die tatsächlich wie rechtlich komplexe Querschnittsmaterie.

Den 1. Teil zu den technischen und wirtschaftlichen Grundlagen leitet *Weiss (Eurocloud Deutschland-eco e.V.)* mit einem Überblick über die Grundbegriffe, Innovationen und Chancen ein, der dem Leser die Euphorie der Bran-

che vermittelt. Danach lenkt *Kittlaus (InnoTivum Consulting)* den Blick auf die wirtschaftlichen Aspekte gängiger Geschäftsmodelle. *Schorer (VMware Global Inc.)* wiederholt Definitionen und Geschäftsmodelle, bevor er auf die technischen Grundlagen und konkrete Angebote eingeht. Mit praxisnahen und detaillierten Übersichten zeigt *Kopanakis (best-practice innovations GmbH)*, was Service-Beschreibungen in Cloud-Verträgen – aus Sicht eines Technikers – leisten müssen.

Im zweiten Teil wenden sich *Intveen, Hilber* und *Rabus* den schuldrechtlichen Beziehungen zwischen Anbietern und Nutzern zu. Sie stellen die Gemeinsamkeiten mit bekannten Outsourcing-Verträgen vor und vertiefen die besonderen Anforderungen an die Vertragsgestaltung. Auf nicht einmal 130 Seiten werden die Vertragsanbahnung, das anwendbare Recht, die Leistungspflichten der Parteien, Mängelrechte und die Vertragsbeendigung abgehandelt. Die Autoren verlieren sich dabei nicht in rechtlichen Details, sondern konzentrieren sich auf die typischen Probleme bei der Auslagerung in die Cloud und überzeugen mit strukturierten Hinweisen für die Gestaltung von Entscheidungsprozessen und Verträgen. Daher fällt es weniger ins Gewicht, dass sie beim Fernabsatzrecht (S. 140 ff.) die durch das Gesetz zur Umsetzung der Verbraucherrechterichtlinie mit Wirkung zum 13.6.2014 in Kraft getretenen Änderungen nicht berücksichtigen konnten (hierzu *Wendehorst*, NJW 2014, 577 ff. und *Raue*, JURA 2015, 326 ff.).

Niemann und Paul – Herausgeber eines eigenen, 2014 erschienenen Praxishandbuchs zum Cloud-Computing (besprochen von *Szalai* UFITA 2015/II, S. 578 ff.) – behandeln im dritten Teil des vorliegenden Werks das Urheberrecht. Nach einem kurzen Abriss der Rechtsquellen kommen die Autoren zur zentralen Vorfrage nach dem kollisionsrechtlich anwendbaren Recht. Sie stellen anschaulich dar, warum das herrschende «Schutzlandprinzip nicht zur digitalen Welt passt» (S. 263; zur Kritik am herrschenden Schutzlandprinzip ausführlich *Schack*, UrhR, 7. Aufl. 2015, Rn. 1012 ff.). Dem Zweck des Handbuchs entsprechend suchen die Autoren die Auswege aus den daraus folgenden Problemen nicht im juristischen Diskurs, sondern wollen den Betroffenen mit technischen Gestaltungen helfen. Zur internationalen Zuständigkeit deutscher Gerichte gehen *Niemann/Paul* auch auf die EuGVVO (VO 44/2001) ein, die indes zum 10.1.2015 von der Brüssel Ia-VO vom 12.12.2012 (VO 1215/2012) abgelöst worden ist. Mit Blick auf den für Urheberrechtsverletzungen einschlägigen deliktischen Gerichtsstand (Art. 7 Nr. 2 Brüssel Ia-VO) diskutieren die Autoren den Erfolgsort der öffentlichen Zugänglichmachung und der Vervielfältigung (S. 271 ff.). Danach stellen sie kurz die für das Cloud-Computing relevanten Schutzgegenstände des Urheberrechts (Software, Datenbanken und Inhalte) vor. Die Nutzungshandlungen leiten sie zutreffend damit ein, dass für

das Cloud-Computing kein unbenanntes Verwertungsrecht (§ 15 II UrhG) angenommen werden muss, weil es schon von den «online-relevanten» Verwertungsrechten (§§ 16 und 19a UrhG) erfasst wird (S. 282 f.). So vielfältige grundsätzlich der Anbieter von SaaS-Diensten die nötige Software, da er die technischen Abläufe auf seinen Servern steuere (S. 285 f.). Der Nutzer vielfältige dagegen meist keine urheberrechtlichen Schutzgegenstände, da allenfalls die Benutzeroberfläche auf seinem Gerät zwischengespeichert werde (S. 286 ff.), die regelmäßig keinen Werkschutz genieße (S. 277). Anders bewerten die Autoren die Lage bei IaaS-Diensten. Hier kontrolliere der Nutzer technische Abläufe und löse deshalb die urheberrechtlichen Nutzungshandlungen aus (S. 292). Nach einem Überblick zu den Schranken gehen die Autoren auf das Lizenzrecht ein. Ob die Verwendung urheberrechtlich geschützter Werke in der Cloud eine eigene Nutzungsart (§ 31 II, III UrhG) ist, beurteilen die Autoren differenzierend mit Blick auf den verwendeten Schutzgegenstand und die Art des Cloud-Dienstes. Die Frage bejahen sie dementsprechend jedenfalls dann, wenn jemand Software im Rahmen eines SaaS-Dienstes nutzt (S. 283 f.). Für den Betrieb eines solchen Dienstes benötige der Provider daher die entsprechenden Nutzungsrechte. Bestehende Netzwerk- oder ASP-Lizenzen sollen hierzu nicht ausreichen (S. 311).

In dem für Anwender wohl wichtigsten vierten Teil befassen sich *Hartung* und *Storm* (*SAP*) mit den datenschutzrechtlichen Fragen. Für die Auslegung entscheidend und richtig ist, dass der Datenschutz in Europa ein «umfassend harmonisierter Rechtsbereich» ist (S. 322, dazu vertiefend *Jotzo*, Schutz personenbezogener Daten in der Cloud, S. 35 ff.). Dass sich – entgegen der Zweifel der Autoren (S. 331) – *Google* und *Facebook* bei entsprechender Auslegung von Art. 3 RL 95/46/EG dem europäischen Recht nicht entziehen können, hat der EuGH mittlerweile entschieden (Rs. C-131/12, EU:C:2014:317 Tz. 42 ff. – *Google Spain*; zur internationalen Anwendbarkeit des europäischen Datenschutzrechts bei Cloud-Diensten ausführlich *Jotzo*, aaO, S. 118 ff.). Mit Blick auf die ausufernde Diskussion um den Personenbezug zeigen *Hartung/Storm*, wie Pseudonymisierung und Verschlüsselung den sachlichen Anwendungsbereich des Datenschutzrechts beeinflussen. Als verantwortliche Stelle stufen sie grundsätzlich den Nutzer ein, der mit der Wahl für einen Cloud-Dienstleister über Zweck und Mittel der Datenverarbeitung iSv. Art. 2 lit. d) der Datenschutzrichtlinie 95/46/EG entscheide (S. 348). Daher muss die Übertragung der Daten von einem Erlaubnisgrund getragen werden, wobei hier im «Normalfall» die Auftragsdatenverarbeitung greife (S. 343). Weiter demonstrieren die Autoren die Schwächen von § 28 BDSG und der Einwilligung (§ 4a BDSG). Für Praktiker besonders wertvoll sind ihre umfangreichen Ausführungen zur Gestaltung der zwischen Nutzer und Anbieter be-

stehenden Auftragsdatenverarbeitung (S. 356 ff.) sowie zu den technischen und organisatorischen Schutzmaßnahmen (S. 372). Da in der Cloud die grenzüberschreitende Datenverarbeitung «eher die Regel als die Ausnahme» ist (S. 405 f.), treten neben die allgemeinen Erlaubnisgründe (1. Stufe) die weiteren Hürden der §§ 4b, 4c BDSG (2. Stufe): Trotz heftiger Diskussionen war die Zertifizierung US-amerikanischer Anbieter nach den Safe-Harbor-Grundsätzen bislang ein wichtiges Instrument, um den Drittstaatentransfer zu rechtfertigen (S. 410 ff.). Nachdem der EuGH jüngst aber die zugrundeliegende Kommissionsentscheidung (2000/520) für ungültig erklärt hat (Rs. C-362/14, EU:C:2015:650 Tz. 98, 104 ff. – Schrems), bleibt abzuwarten, welchen Ersatz die Politik liefern wird. Zumindest kurzfristig werden nach dem EuGH-Urteil die Standardvertragsklauseln für Auftragsdatenverarbeiter (Beschluss der Kommission 2010/87/EU) wichtiger, deren Probleme beim Einsatz durch Cloud-Anbieter *Hartung/Storm* darstellen (S. 413 ff.). Zudem diskutieren sie breit, ob § 3 VIII 3 BDSG den Einsatz außereuropäischer Auftragsdatenverarbeiter verhindert, was bei richtlinienkonformer Auslegung nach Art. 17 RL 95/46/EG (S. 417) nicht der Fall ist (*Jotzo*, aaO, S. 148 ff.). Den datenschutzrechtlichen Teil beschließen *Hartung/Storm* mit einem Überblick über die Betroffenenrechte und die Folgen von Datenschutzverstößen.

Anschließend behandelt *Hexel* individual- und kollektivarbeitsrechtliche Fragen, die sich Unternehmen bei der Einführung von Cloud-Lösungen stellen (5. Teil). Nach einem Abriss der Rechtsquellen und deren internationaler Anwendbarkeit zeigt *Hexel*, dass Arbeitnehmer die Einführung von Cloud-Diensten regelmäßig dulden müssen, soweit Arbeitgeber sich auf ihr Direktionsrecht stützen (S. 445). Unterrichts- und Fortbildungsansprüche können in dieser Situation die Interessen der Arbeitnehmer wahren (S. 446 ff.). Anschließend geht *Hexel* auf die Möglichkeiten betriebsbedingter Kündigungen und die Arbeitnehmerrechte beim Betriebsübergang (§ 613a BGB) ein. Im Unterschied zu klassischen Outsourcing-Projekten ist der Betriebsübergang beim Einsatz von Cloud-Systemen aber praktisch die Ausnahme und nur bei «größeren Vorhaben» vorstellbar (S. 459). Für das Cloud-Outsourcing wichtiger und gern übersehen wird vielmehr, dass Cloud-Dienste oft auch Daten der Beschäftigten verarbeiten, sodass Arbeitgeber dem Betriebsrat «häufig sehr detaillierte und umfassende Informationen» über die Anwendungen liefern müssen, § 80 I Nr. 1 BetrVG (S. 464). Auch kann die Einführung von Cloud-Systemen der Mitbestimmung (§ 80 I Nr. 1 und Nr. 6 BetrVG) unterliegen und Beratungsrechte (§ 90 BetrVG) auslösen (S. 466 ff.).

Rechtsanwalt und Steuerberater *Knorr* betrachtet im sechsten Teil die steuerlichen Folgen des Nutzens und Anbietens von Cloud-Diensten. Ausführlich geht er zunächst auf die Ertragssteuer ein und sucht nach möglichen Betriebs-

stätten als Anknüpfungspunkt der inländischen Steuerpflicht. Danach zeigt er praxisnah, welche Grenzen handels- und steuerrechtliche Aufbewahrungspflichten den Unternehmen setzen, die Cloud-Lösungen für ihre Unternehmenskommunikation oder Buchführung einsetzen wollen. Der letzte Abschnitt ist der Umsatzsteuer gewidmet.

Im siebten Teil befassen sich *Trüg* und Prof. *Mansdörfer* mit den straf- und strafprozessrechtlichen Aspekten. Spannend sind ihre Ausführungen zum Zugriff der Strafverfolgungsorgane auf Server im Ausland auf Grundlage von Rechtshilfeersuchen und der Cyber-Crime-Convention (BGBl. 2008 II, 1242). Die praktische Bedeutung solcher grenzüberschreitenden Strafverfolgungsmaßnahmen belegt nicht zuletzt der Fall *Microsoft*, in dem sich das Unternehmen vor einem New Yorker Gericht gegen die Herausgabe von Daten an US-Strafverfolgungsbehörden wehrte, die auf Cloud-Servern in Irland gespeichert waren (ZD 2014, 346 ff. m. Anm. *Schröder/Spies*). Die Autoren stellen anschaulich dar, welche personellen und organisatorischen Strukturen Cloud-Anbieter schaffen sollten, um auf Behördenanfragen bei Ermittlungen gegen Nutzer rechtmäßig zu reagieren. Weiter gehen sie auf die Grenzen ein, die das Strafrecht – insbesondere die Verletzung von Privatgeheimnissen (§ 203 StGB) – den Nutzern setzen, die Daten in die Cloud auslagern wollen.

Der achten Teil gilt den Besonderheiten «regulierter Märkte». Einleitend betrachtet *Ulmer* (Konzerndatenschutzbeauftragter der *Deutschen Telekom AG*) das TK- und Telemedienrecht. Dass er deren internationale Anwendbarkeit gleich zweimal (S. 584 f. und 608 f.) und die Zugriffsmöglichkeiten der Strafverfolger erneut (7. Teil) behandelt (S. 609 ff.), irritiert. Auch hätte er auf S. 595 deutlicher machen sollen, dass die Haftungsprivilegierungen der §§ 7 ff. TMG, aufgrund europäischer Vorgaben, nicht bei Datenschutzverstößen gelten (*Spindler/Schuster-Hoffmann*, Recht der elektronischen Medien, 3. Aufl. 2015, vor §§ 7 ff. TMG, Rn. 14). *Glaus* und *Horras* zeigen dann informativ und prägnant, welche Probleme das Bankaufsichtsrecht bereiten kann. Eingehend befassen sie sich mit § 25a KWG und dem Auslagerungsverhältnis nach den Mindestanforderungen an das Risikomanagement (*BaFin*, Rundschreiben 10/2012). Anschließend gehen sie darauf ein, wie Finanzinstitute bei der Auslagerung das Bankgeheimnis wahren. *Erben (SAP)* führt weiter in vergaberechtliche Aspekte ein, die öffentliche Auftraggeber und Bieter beachten sollten. *Hartung* wiederholt (7. Teil) und vertieft den Tatbestand des Geheimnisverrats. Ausführlich stellt er technische und organisatorische Lösungen vor, trotz derer Geheimnisverpflichtete iSv. § 203 StGB Cloud-Systeme «nur unter Einschränkungen» einsetzen können (S. 730). Danach zeigt *Bieresborn* (Richter am Bundessozialgericht), welche Probleme der Sozialdatenschutz bei der Auslagerung von Verarbeitungsprozessen durch öffentliche Sozialleistungsträ-

ger und private Leistungserbringer bereitet. *Müller* rundet den achten Teil mit einem gut verständlichen Abschnitt über das Exportkontrollrecht ab. Darin behandelte er vor allem die Grenzen, die Cloud-Nutzer beachten müssen, die exportrechtlich relevante Daten in der Cloud verarbeiten wollen, etwa solche für die Herstellung exportkontrollierter Güter (S. 761).

Vor allem Praktiker werden zu diesem Handbuch greifen, das mit seinen zahlreichen Gestaltungshinweisen für Verträge, Verfahrensabläufe und Organisationsstrukturen überzeugt. *Hilber* und sein Autorenteam stellen in weiten Teilen prägnant die ganze Breite juristischer Themen der Cloud vor. Sie behandeln eingehend die speziellen Herausforderungen, die diese neue Outsourcing-Alternative den Rechtsanwendern bereitet. Dieser Fokus rechtfertigt den Platz, den das Werk auch künftig, neben den etablierten Standardwerken aus derselben Reihe von *Schneider* (EDV Recht, 5. Aufl. 2016) und *Härting* (Internetrecht, 5. Aufl. 2014), haben wird. Seiner Eigenschaft als Handbuch würde es aber nicht schaden, wenn die Autoren in künftigen Folgeauflagen die juristische Diskussion in den Fußnoten umfassender nachweisen. Dann entstünde nicht nur ein praxisnaher und profunder Überblick, sondern zugleich ein wertvoller Einstieg in die lebhaft geführten Auseinandersetzungen zu einem faszinierenden Thema, deren Kenntnis auch im Alltag praxisrelevant werden kann.

Wiss. Mitarbeiter Dr. *Florian Jotzo*, Kiel

Schumacher, Fee: Urheberschutz für Regieleistungen im Theater. Studien zum Gewerblichen Rechtsschutz und zum Urheberrecht Bd. 121, Verlag Dr. Kovač, Hamburg 2015, 238 S., ISBN 978-3-8300-8193-7, € 88.90

Erfreulich ist, dass sich die Arbeit erneut mit einem Thema beschäftigt, dessen Probleme bis heute nicht gelöst sind. Das betrifft vor allem die Rechtsstellung des Theaterregisseurs. Die Dissertation wurde von *Karl-Nikolaus Peifer* betreut. *Schumacher* sieht die Gefahr, in ausgetretenen Pfaden zu wandeln und wenig wissenschaftlich beitragen zu können. Diese Gefahr besteht immer, aber die Arbeit offenbart eine große Spielwiese unterschiedlicher inhaltlicher und methodischer Aspekte, die teilweise über Bekanntes hinausgehen. Die Arbeit gliedert sich in fünf Kapitel. Der Untersuchung werden zwei Fragestellungen vorangestellt, die den Kern der Arbeit bilden. Erstens: Erlangt der Theaterregisseur grundsätzlich ein Bearbeiterurheberrecht nach § 3 UrhG an der durch seine Regieleistung entstandenen Inszenierung? Zweitens: Liegt dieses Urheberrecht auch im Interesse der Regisseure, da es bei einer ausschließlichen Anwendung von Leistungsschutzrechten zu Rechtsschutzlücken kommen