Magda Wicker: Cloud Computing und staatlicher Strafanspruch. Strafrechtliche Risiken und strafprozessuale Ermittlungsmöglichkeiten in der Cloud

von Prof. Dr. Anja Schiemann

2016, Verlag Nomos, Baden-Baden, ISBN: 978-3-8487-2776-6, S. 503, Euro 129,00.

Rechtsfragen rund um das Thema Cloud Computing beschäftigen schon seit einigen Jahren die juristische Fachwelt. Die vorliegende Dissertation zu strafrechtlichen und strafprozessualen Aspekten stammt von keiner Unbekannten. Vielmehr hat *Wicker* schon viele Fachaufsätze verfasst und u.a. zu der – meines Erachtens vorschnellen und falschen – Einschätzung in der Kommentierung von *Meyer-Goßner/Schmitt* beigetragen, der Zugriff auf ein externes Speichermedium außerhalb Deutschlands vom Computer des betroffenen Cloud-Nutzers über dessen Account sei von § 110 Abs. 3 StPO als rechtmäßige Ermittlungshandlung im Inland gedeckt (StPO, 59. Aufl. [2016], § 110 Rn. 7b). Von daher durfte man mit Spannung erwarten, wie sich *Wicker* den unterschiedlichen materiellrechtlichen und prozessualen Themen mit Bezug auf das Cloud Computing nähert und positioniert. Die Arbeit ist sehr umfangreich und gliedert sich in sechs Kapitel. Hilfreich wäre es angesichts des Umfangs von 500 Seiten gewesen, wenn die jeweiligen Erkenntnisse am Ende eines Kapitels zusammengefasst worden wären. Eine solche Zusammenfassung findet sich jedoch weder in den Kapiteln noch als Ergebniszusammenfassung am Ende der Monografie. Erschwert wird die Orientierung durch unpräzise Inhaltsangaben, wie bei Kapitel 3, in dem zwar die Unterabschnitte benannt, diese jedoch jeweils als „Kapitel 0“ bezeichnet werden (S. 63). Hier hätte mehr Wert auf eine redaktionelle Endbearbeitung gelegt werden sollen.

Nach einer Einleitung widmet sich *Wicker* im zweiten Kapitel den technischen und wirtschaftlichen Grundlagen des Cloud Computings sowie den Chancen und Risiken für mittelständische Unternehmen und für den öffentlichen Sektor (S. 35 ff.). Des Weiteren wird der Untersuchungsgegenstand der Arbeit abgesteckt und das „übliche Speichern in der Cloud zugrunde gelegt“ (S. 60). Außerdem wird davon ausgegangen, dass die Cloud sich auf Servern im In- oder Ausland befinden kann und weder Cloud-Nutzer noch Cloud-Anbieter zu einem bestimmten Zeitpunkt Kenntnis vom aktuellen Speicherort haben. Allerdings sei es dem Cloud-Anbieter möglich, den jeweiligen Speicherort nachträglich herauszufinden. Einschränkend wird zudem festgelegt, dass ausschließlich deutsches Recht berücksichtigt wird.

Das dritte Kapitel nimmt eine rechtliche Einordnung des Cloud Computings vor (S. 63 ff.). Im Rahmen einer knappen zivilrechtlichen Auseinandersetzung wird von einem mietrechtlichen Vertragsverhältnis ausgegangen und dieses kurz skizziert. Es folgt eine medienrechtliche Einordnung nach dem TKG und TMG. Schließlich bezeichnet *Wicker* ihren rechtlichen Untersuchungsgegenstand des Cloud Computings als „Datenspeichermiete“ (S. 96).

Nach diesen grundsätzlichen Ausführungen folgt ein mit 180 Seiten sehr umfangreiches Kapitel zu den strafrechtlichen Risiken beim Cloud Computing (S. 99 ff.). Untersucht werden die potentiell einschlägigen Vorschriften im Strafgesetzbuch sowie dem Nebenstrafrecht. Unterteilt wird jeweils pro Delikt nach möglicher Strafbarkeit des Cloud-Anbieters, des Cloud-Nutzers sowie möglicher Angreifer. Es geht der Verfasserin um die Identifizierung von Strafbarkeitsrisiken der Cloud-Akteure, wobei die Tatbestandsmerkmale extensiv ausgelegt werden, um alle potentielle Strafbarkeitsrisiken zu erfassen (S. 103).

Eine Strafbarkeit wegen Verletzung des Briefgeheimnisses nach § 202 StGB lehnt *Wicker* mangels Verkörperung der Inhaltsdaten beim Cloud Computing ab. Eine Strafbarkeit wegen des Ausspähens von Daten gem. § 202a StGB käme allerdings für den Cloud-Anbieter oder Dritten in Betracht. Eine extensive Auslegung des Tatbestands stelle auf den Missbrauch der tatsächlichen Zugriffsmöglichkeiten des Cloud Anbieters als Administrator ab. Sofern der Cloud-Anbieter technisch notwendig handele, bestehe dagegen kein Strafbarkeitsrisiko. Hinsichtlich der Strafbarkeit wegen des Abfangens von Daten gem. § 202b StGB differenziert die Verfasserin zwischen Datenup- und Download sowie Cloud Sharing. Während ersteres bei Erfüllung der weiteren Voraussetzungen vom Straftatbestand erfasst sein könne, würden Fälle des Cloud Sharings nicht unter den Tatbestand fallen. Den Straftatbestand des Vorbereitens des Ausspähens und Abfangens von Daten gem. § 202c StGB könne der Cloud-Anbieter bei entsprechendem objektiven und subjektiven Verhalten begehen. Allerdings stelle allein der Aufbau eines Cloud-Angebots einschließlich der späteren Möglichkeit, auf Daten zugreifen zu können, keine vorwerfbare Handlung dar. Lediglich dann, wenn der Cloud-Anbieter in der Absicht, Daten von Cloud-Nutzern „abgreifen“ zu können, seine Cloud einrichtet und aufbaut, könne er den Straftatbestand des § 202c StGB verwirklichen.

Die größten Strafbarkeitsprobleme sieht *Wicker* in der Verletzung von Privatgeheimnissen gem. § 203 StGB. Die

Nutzung einer Cloud ohne starke technische Sicherungsmaßnahmen stelle für die im Straftatbestand genannten Berufsgruppen eine Geheimnisoffenbarung dar. Für die allermeisten Fälle dürfe die Einwilligung der Patienten oder Mandanten zur Geheimnisoffenbarung im Rahmen des Cloud Computings nicht mutmaßlich angenommen werden (S. 143). Im Anschluss daran prüft die Verfasserin eine Strafbarkeit wegen Verwertung fremder Geheimnisse nach § 204 StGB und verneint eine Strafbarkeit in allen aufgezeigten Konstellationen. Entweder fehle es an einer Schädigungsabsicht des Berufsgeheimnisträgers oder an der Sonderstellung des Cloud-Anbieters. Ausführlich prüft *Wicker* dann die Strafbarkeit der Verletzung des Post- oder Fernmeldegeheimnisses gem. § 206 StGB. Für den Cloud-Anbieter verneint sie eine Strafbarkeit, da dieser weder Inhaber noch Beschäftigter eines Unternehmens sei, das geschäftsmäßig Telekommunikationsdienste erbringe. Nur Inhaber, Vertreter oder Beschäftigte von originären Telekommunikationsunternehmen könnten sich bei der Cloud-Nutzung nach § 206 StGB strafbar machen, sofern eine Datenverarbeitung oder eine unverschlüsselte Speicherung von Daten, die dem Fernmeldegeheimnis unterliegen, in der Cloud durchgeführt wird (S. 174).

Wegen Datenveränderung nach § 303a StGB können sich lediglich der Cloud-Anbieter oder Dritte strafbar machen. Der Cloud-Anbieter habe ebenso wie der Dritte keine Verfügungsberechtigung über die Daten seiner Cloud-Nutzer, so dass diese fremd und somit taugliches Tatobjekt seien. Der Cloud-Anbieter könne sich demzufolge strafbar machen, wenn er Daten des Cloud-Nutzers in der Cloud löscht oder den Zugang sperrt. Eine Strafbarkeit entfalle nur dann, wenn technische Gegebenheiten oder vertragliche Vereinbarungen dies rechtfertigen. Laut *Wicker* können sich sowohl der Cloud-Anbieter, als auch der Cloud-Nutzer und Dritte der Computersabotage gem. § 303b StGB strafbar machen. Die Tatvariante des § 303b Abs. 1 Nr. 1 StGB scheide für den Nutzer allerdings aus, weil es dort auf die Fremdheit in Form der fremden Datenverfügungsbefugnis ankomme.

Während ein nennenswertes Strafbarkeitsrisiko im Anwendungsbereich des Cloud Computings hinsichtlich der Zerstörung wichtiger Arbeitsmittel gem. § 305a StGB nicht bestehe, berge Cloud Computing ein Risiko hinsichtlich der Strafbarkeit gem. § 353b StGB. Die Verletzung von Dienstgeheimnissen und einer besonderen Geheimhaltungspflicht könne zahlreiche Personen der öffentlichen Verwaltung treffen. Dagegen komme eine Strafbarkeit des Cloud-Nutzers wegen verbotener Mitteilungen über Gerichtsverhandlungen gem. § 353d Nr. 1 und Nr. 3 StGB nicht in Betracht, da das Merkmal der öffentlichen Mitteilung aufgrund eines publizierenden Aspekts nicht durch die schlichte Cloud-Nutzung erfüllt werden könne. Dagegen könne eine unbefugte Offenbarung gem. § 353d Nr. 2 StGB gegeben sein, wenn im Falle eines Gerichtsbeschlusses gem. § 174 Abs. 3 GVG der Schweigepflicht unterliegende Tatsachen einer Gerichtsverhandlung oder Inhalte eines die Sache betreffenden amtlichen Schriftstücks in die Cloud eingebracht werden. Als Täter komme dabei allerdings nur derjenige in Betracht, dem persönlich eine Schweigepflicht auferlegt worden ist. Für besonders Verpflichtete i.S. des § 355 StGB bestehe zudem ein Strafbarkeitsrisiko der Verletzung des Steuergeheimnisses bei der Cloud-Nutzung. Dagegen schaffe die Nutzung von inländischen Cloud-Angeboten kein Strafbarkeitsrisiko gem. §§ 94, 95 StGB, da es nicht nur auf die Möglichkeit der Kenntnisnahme durch Dritte ankomme. Jedoch bestehe bei Nutzung US-amerikanischer Cloud-Angebote im Zusammenhang mit Staatsgeheimnissen ein Strafbarkeitsrisiko nach §§ 94, 95 StGB. Danach prüft *Wicker* relevante Strafnormen außerhalb des StGB, und zwar im BDSG und § 17 UWG (S. 230 ff.).

Im Anschluss daran findet sich an versteckter Stelle und nicht abschließend für das Kapitel eine Zusammenfassung der Strafbarkeitsrisiken der Cloud-Akteure (S. 252 ff.), die wiederum nach Cloud-Nutzer, Cloud Anbieter und Drittem differenziert. In einem weiteren Unterabschnitt „Speichern in der Cloud – ohne strafrechtliche Risiken“ (S. 259 ff.), gibt die Autorin eine Risikobewertung ab und zeigt Möglichkeiten einer Vermeidung der Strafbarkeit auf. Dieser Unterabschnitt ist leider recht knapp gehalten, die Erkenntnisse knüpfen zwangsläufig an der vorigen ausführlichen Strafbarkeitsprüfung an. Übersichtlicher wäre es sicher gewesen, schon im Unterabschnitt der Strafbarkeitsprüfung mehr zu clustern, um so einen systematischen Überblick zu geben. Dieser hätte dann, eventuell in Tabellenform, auch bei den Empfehlungen der Autorin die Strukturen deutlicher gemacht und die Rechtsprobleme klarer.

Im fünften Kapitel widmet sich *Wicker* den strafprozessualen Ermittlungen beim Cloud Computing (S. 281 ff.). Nach einer Darstellung allgemeiner Grundsätze der Beweisführung im Strafprozess in Bezug auf Daten, geht es sodann detailliert um die Möglichkeiten der Strafprozessordnung im Zusammenhang mit der Cloud-Nutzung. In diesem Kapitel bekräftigt die Autorin z.B. ihre Auffassung zur Durchsicht externer Speichermedien nach § 110 Abs. 3 StPO, eine Beschränkung auf inländische Festplatten ergäbe sich weder aus dem Wortlaut noch aus anderen Gesichtspunkten. Schuldig bleibt *Wicker* insofern – zunächst – die Antwort auf die Frage, warum sich dann in der Cybercrime Convention überhaupt solche Mühe gemacht wird, grenzübergreifende Zugriffe zu regeln bzw. wie völkerrechtliche Gesichtspunkte hier rechtlich relevant werden oder etwa nicht. Wer hier eine Vertiefung ihres in Aufsätzen vertretenen Standpunkts erwartet, wird leider enttäuscht. Im Hinblick auf die Beschlagnahme sieht die Autorin weniger rechtliche als vielmehr praktische Probleme, da der Zugriff beim Cloud-Nutzer primär am Zugang scheitern werde. Allerdings könne der Zugriff beim Cloud-Anbieter in einem größeren Umfang erfolgen, als vom Beschlagnahmebeschluss vorgesehen. Wünschenswert wäre es daher, dass der Cloud-Anbieter die Grenzen der Beschlagnahmeanordnung wahrt und nicht die Einrichtung eines Gastzugangs für die Ermittlungsbehörden ermöglicht, sondern die Daten nur im Umfang der Beschlagnahmeanordnung herausgibt.

Telekommunikationsüberwachung gem. §100a StPO bzgl. der Übermittlung von Daten zwischen dem Cloud-

Anbieter und Cloud-Nutzer hält *Wicker* zwar für technisch denkbar, jedoch als heimliche Maßnahme für rechtlich nicht möglich. Auch die Bestandsdatenauskunft nach § 100j StPO und die Verkehrsdatenauskunft gem. § 100g StPO seien keine geeigneten Maßnahmen bei Ermittlungen in der Cloud. Die Ermittlungsgeneralklausel scheide für einen Zugriff auf Daten in der Cloud ebenfalls aus. Lägen Zugangsdaten vor, so könnten allerdings gem. § 102 StPO im Wege einer Durchsuchung innerhalb der Daten des Cloud-Nutzers die Ermittlungen fortgesetzt werden.

Im Anschluss an diese Ergebnisse benennt *Wicker* noch einmal die strafprozessualen Zugriffsmöglichkeiten bei den Cloud-Akteuren und differenziert nach Cloud-Nutzer, Cloud-Anbieter, Ermittlungen im Internet und Ermittlungen im Ausland. Einige Ausführungen sind redundant zu den vorherigen, andere werden näher ausgeführt, so dass sich der Leser fragt, warum nicht schon zuvor mehr in die Tiefe gegangen wurde. So folgen z.B. beim Unterpunkt „Ermittlungen beim Cloud-Nutzer vor Ort – Daten der reinen Cloud“ wiederum Ausführungen zu § 110 StPO und ausländischen Speichermedien. Hier wird jetzt explizit auch auf die Cybercrime-Convention Bezug genommen, deren Relevanz sich auch schon im Unterkapitel zuvor ergeben hätte. Zudem wird später noch einmal unter dem Punkt „Ermittlungen im Ausland“ auf die gleiche Problematik eingegangen. Diese Zersplitterung der jeweils gleichen Rechtsmaterie ist nicht nur redundant, sondern durch Auslassungen an der einen und Vertiefungen an der anderen Stelle für den Leser auch nicht in Gänze nachvollziehbar. Hier zeigt sich – wieder einmal, – dass der Aufbau nur bedingt geglückt ist.

Im sechsten Kapitel widmet sich *Wicker* dem straf-(prozess-)rechtsverträglichem Cloud Computing (S. 445 ff.). Dazu werden die gefundenen Ergebnisse zunächst für eine rechtsverträgliche Gestaltung von Cloud Computing aufbereitet und Empfehlungen für kleinere und mittlere Unternehmen sowie den öffentlichen Sektor gegeben. Dabei ist die Empfehlung für Cloud-Nutzer und Cloud-Anbieter, Strafbarkeitsrisiken zu vermeiden, recht trivial. Allerdings zeigt sich hier der Nutzen der Ausführungen zum materiellen Recht, die hier noch einmal kurz zusammengetragen werden und zum Hinweis von Risikovermeidungsstrategien führen. Dies ist sicher wertvoll, gleitet aber leider teilweise in banale Feststellungen ab. So wird für Cloud-Nutzer, die das Datenschutzrecht beachten müssen, der Tipp gegeben, „die datenschutzrechtlichen Vorgaben zur Cloud-Nutzung einzuhalten“ (S. 453).

Handlungsbedarf in Sachen Cloud Computing sieht *Wicker* nur im Bereich der besonders Geheimnisverpflichteten, weist insoweit aber auf gesetzgeberische Aktivitäten des BMJV hin. Mittlerweile liegt ein Regierungsentwurf des Gesetzes zur Neureglung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vor (BT-Drs. 18/11936). Ansonsten hält die Autorin Änderungsbedarf de lege ferenda für nicht erforderlich, sondern zieht resümierend das Fazit, sowohl das Strafgesetzbuch als auch die Strafprozessordnung könnten der Ära „Cloud“ standhalten (S. 472).

Ob dieses Fazit überzeugt, mag jeder, der die Dissertation oder die einschlägigen Kommentierungen zu den entsprechenden Strafnormen oder strafprozessualen Ermächtigungsgrundlagen liest, selbst beurteilen. Fest steht jedenfalls, dass die zunehmende Digitalisierung bestenfalls zu Auslegungsschwierigkeiten, schlimmstenfalls zu dem Dilemma führt, neue Sachverhalte in veraltete Vorschriften pressen zu wollen. Ermittlungen in der Cloud stellen die Strafverfolgungsbehörden vor immer größere Anforderungen – dies nicht nur in rechtlicher, sondern auch in ermittlungstaktischer Hinsicht. Einen guten Überblick über strafrechtliche und strafprozessuale Implikationen gibt hier die Dissertation von *Wicker*.