B u c h r e z e n s i o n

Magda Wicker, Cloud Computing und staatlicher Strafanspruch. Strafrechtliche Risiken und strafprozessuale Ermittlungsmöglichkeiten in der Cloud, Nomos, Baden-Baden, 2016, 503 S., € 129,-.

Die Monographie mit dem Titel „Cloud Computing und staatlicher Strafanspruch" von *Magda Wicker* enthüllt ihren Inhalt erst im Untertitel. Denn wo der Titel zunächst nur eine Abhandlung über die materiell-rechtlichen Folgen des Cloud Computing erahnen lässt, liefert *Wicker* darüber hinaus auch eine Untersuchung der strafprozessualen Problematiken in diesem Umfeld. Dies geschieht nicht ohne zuvor die technischen Grundlagen sowie die zivil-, und medienrechtliche Einordnung des Cloud Computing zu erläutern. Dabei dürfte der Umstand, dass das Werk von *Wicker* im Rahmen zweier Forschungsprojekte entstand, die sich interdisziplinär mit der Praktikabilität und Sicherheit von Cloud Computing beschäftigten, für die umfassende Perspektive und das erkennbare technische Hintergrundwissen der *Autorin* förderlich gewesen sein. Der Leser bekommt somit ein thematisches Komplettpaket zum Thema Cloud Computing und Strafrecht geliefert, was sich auch im – für eine Dissertationsschrift recht stattlichen – Umfang niederschlägt.

Im Aufbau geht *Wicker* stringent vor. Zunächst werden in einem ersten Kapitel (S. 23-34) neben einer Einleitung die grundlegenden Informationen zum Werk wie z.B. Stand der Forschung (S. 28) oder Rahmen und Methodik der Untersuchung (S. 26 bzw. 30) erläutert. Die technischen Hintergründe, soweit zum Verständnis des Werkes notwendig, sind im zweiten Kapitel (S. 35-62) dargelegt. Die juristische Auseinandersetzung beginnt sodann im dritten Kapitel (S. 63-98) mit der erwähnten rechtlichen Einordnung des Cloud Computings im Zivil- und Medienrecht. Die materiell-strafrechtlichen Risiken im Rahmen des Cloud Computings werden im vierten Kapitel (S. 99-280) untersucht. Die Folgen für das Strafprozessrecht sind im fünften Kapitel (S. 281-444) dargelegt. Die Ergebnisse und Schlussfolgerungen aus dem Vorhergenannten fasst *Wicker* im sechsten und letzten Kapitel (S. 445-472) nochmals konzentriert zusammen.

Im ersten Kapitel ist die Darstellung des methodischen Vorgehens besonders erwähnenswert. Hier stellt *Wicker* heraus, dass im späteren materiell-strafrechtlichen Teil insbesondere untersucht werden soll, welche Strafbarkeitsrisiken sich aus der Nutzung von Cloud Computing für die beteiligten Akteure ergeben können (S. 30). Strafbarkeitsrisiken meint dabei die mögliche Strafbarkeit von Verhaltensweisen im Zusammenhang mit Cloud Computing, die nach der weitesten zulässigen Auslegung der Tatbestände denkbar ist. Gleichwohl, darauf sei schon jetzt hingewiesen, stellt *Wicker* in der Bearbeitung der einzelnen Tatbestände auch die ihrer Ansicht nach zutreffende Auslegung dar.

Von grundlegend wichtiger Bedeutung für das weitere Vorgehen sind die Ausführungen im zweiten Kapitel. *Wicker* stellt hier verschiedene vorhandene Definitionsansätze für Cloud Computing vor (S. 38 ff.) und stellt deren besondere Merkmale heraus. Dabei greift sie neben den nationalen Ansätzen, etwa des BSI (S. 39), vor allem auch auf die in diesem Kontext wohl maßgeblichen Beschreibungen aus dem US-amerikanischen Raum zurück. Im Ergebnis identifiziert *Wicker* verschiedene Merkmale, die Cloud Computing erfüllen muss (S. 40). Danach ist, grob zusammengefasst, Cloud Computing als ein IT-Bereitstellungsmodell zu verstehen, bei dem der Cloud-Nutzer auf die Beschaffung eigener Hard- und/oder Software verzichtet und stattdessen auf die ständig zu diesem Zweck bereitgestellten Ressourcen des Cloud-Anbieters zurückgreift. Insbesondere die Virtualisierung, die Skalierbarkeit und der Bezug über das Internet seien wesentliche Merkmale (vgl. S. 40-43). Neben der Definition werden auch der Stand der Technik sowie die gängigen Modelle dargestellt, in denen Cloud Computing erfolgt. *Wicker* versteht es hierbei, technische Begriffe und Kürzel (z.B. SaaS, PaaS, IaaS etc.) auch für den Laien verständlich aufzubereiten und zu erläutern.

Nach der technischen Einführung widmet sich die *Autorin* der juristischen Aufarbeitung des Cloud Computings. Dabei erfolgt die Einordnung in zivilrechtlicher Hinsicht (S. 65-83) nicht zum Selbstzweck. Das gefundene Ergebnis wird in der späteren Bearbeitung der straf- und strafprozessrechtlichen Ebene immer wieder aufgegriffen und argumentativ genutzt. *Wicker* dekliniert verschiedene im besonderen Schuldrecht kodifizierte Vertragstypen durch und kommt zu dem Ergebnis, dass es sich bei Cloud Computing weder um einen Kauf-, noch einen Dienst- oder Werkvertrag handelt. Vielmehr sei das Bereitstellungsmodell als Mietvertrag einzuordnen (S. 71). Der Cloud-Nutzer beanspruche die Ressourcen des Cloud-Anbieters, welche dieser ihm auch in dem vertraglich vereinbarten Maße zum Gebrauch gewähre. Die Einordnung wird anhand der Rechtsprechung zu ähnlichen Fragestellungen verifiziert und gelingt argumentativ überzeugend. So sei beispielsweise durch den Mietvertrag lediglich die Gebrauchsüberlassung geschuldet. Der Umstand, dass der Cloud-Nutzer keinen Besitz an der genutzten Hardware erhalte, sei in diesem Zusammenhang irrelevant, da bei IT-Systemen der Gebrauch über den Weg des Internets die Besitzverschaffung nicht erfordere (S. 74). Gerade dieses Merkmal (Virtualisierung) unterscheide andere und vertragstypologisch abweichend eingeordnete Absprachen wie z.B. den Webhostingvertrag.

Im Rahmen der medienrechtlichen Einordnung (S. 83-89) erläutert *Wicker* auf Basis der technischen Definition, dass eine Anwendung des TKG auf Cloud Computing nicht möglich sei. Dies begründe sich aus dem Umstand, dass Telekommunikationsdienste zwar für den Up- bzw. Download beim Cloud Computing benötigt werden, sie aber gerade nicht Teil des Cloud Computing-Vertrages sind. Eine Kommunikation finde bei der reinen Übertragung von Daten des Cloud-Nutzers zu der gemieteten Infrastruktur und zurück gerade nicht statt. Anders sei die Lage in Bezug auf das TMG zu bewerten. Der Cloud-Anbieter erfülle die Voraussetzungen des § 2 S. 1 Nr. 1 TMG. In diesem Zusammenhang sei zwischen Bestands-, Nutzungs- und Inhaltsdaten zu unterscheiden, deren Einordnung und Voraussetzungen im Einzelnen dargestellt werden.

Nach diesen detaillierten Vorarbeiten wird nach den dargestellten Grundsätzen auf die bestehenden Strafbarkeitsrisiken eingegangen, denen sich Cloud-Nutzer, Cloud-Anbieter und Dritte gegenübersehen. *Wicker* geht auch hier umfassend vor. Dabei nimmt sie zunächst die Straftatbestände des StGB und im Anschluss die der relevanten Nebengesetze (wie z.B. des UWG) in den Blick. Um nicht den Rahmen einer Rezension zu sprengen, sei hier nur auf einige wenige Tatbestände hingewiesen. Eine umfassende Zusammenfassung der möglichen Strafbarkeitsrisiken findet sich, aufgeschlüsselt nach den jeweiligen Akteuren, auf den Seiten 252-280.

Wenig überraschend nimmt *Wicker* zunächst § 202a StGB in den Blick. Sie stellt klar, dass die Abreden im Cloud-Vertrag keine Berechtigung des Cloud-Anbieters enthalten, die in der Cloud gespeicherten Daten auszulesen oder zu verändern (S. 107). Dies sei auch bei technisch notwendigen Zugriffen oder vereinbarten Sicherungskopien der Fall, weil hierfür ein inhaltlicher Zugriff nicht erforderlich sei (S. 108). Interessant ist die Beantwortung der Frage, ob die Daten des Cloud-Nutzers gegenüber dem Zugriff des Cloud-Anbieters i.S.d. § 202a StGB besonders gesichert sind. Eine solche Sicherung sei regelmäßig durch das Nutzerkennwort gegeben, welches aber dem Cloud-Anbieter in Klarform oder als zum Inhaltszugriff nutzbarer Hashwert zur Verfügung stehe (S. 112). *Wicker* kommt mittels einer Analogie zur realen Welt zu dem Schluss, dass ein Nutzerkennwort dennoch für den § 202a StGB tatbestandlich ausreiche. Ebenso wie ein Vermieter einen Schlüssel zu dem Mietobjekt behalten könne, er in der Anwendungsbefugnis aber aufgrund des Mietvertrages beschränkt sei und sich bei vertraglich nicht genehmigtem Betreten strafbar machen könne, sei dies auch bei dem Cloud-Anbieter der Fall, wenn er vertragswidrig das ihm bekannte Passwort zur Einsichtnahme in die Daten nutze (S. 113 f.). Im Ergebnis sei ein Strafbarkeitsrisiko des Cloud-Anbieters bei einer solchen Einsichtnahme zu bejahen.

Einen für die Praxis besonders relevanten Tatbestand im Zusammenhang mit Cloud Computing nimmt *Wicker* in Form des § 203 StGB in den Blick. Es stellt sich hier die Frage, ob die Speicherung etwa von Mandanten- oder Krankenakten sowie Verfahrensakten verschiedener Behörden in der Cloud den Tatbestand erfüllen könnte. Die *Autorin* sieht ein Offenbaren nach dieser Vorschrift bereits dann als gegeben an, wenn die Möglichkeit der Kenntnisnahme des Geheimnisses gegeben ist. Dies ist zwar nicht unumstritten, vor dem Hintergrund der Aufdeckung von Strafbarkeitsrisiken jedoch folgerichtig. Durch die Speicherung in der Cloud und der damit einhergehenden technischen Möglichkeit des Cloud-Anbieters, vertragswidrig in die Daten Einsicht zu nehmen, sei der Tatbestand an sich erfüllt. Dies ließe sich nur durch eine Sicherung auf dem Stand der Technik, insbesondere durch Verschlüsselungslösungen umgehen (S. 133). Hier lässt sich auch exemplarisch die Praxisrelevanz des Werkes erkennen, indem *Wicker* auf die daraus folgenden Umsetzungsprobleme hinweist. So ist eine Verarbeitung der Daten, anders als eine reine Speicherung, im Wege des Cloud Computing (z.B. mittels Software as a Service/SaaS) derzeit im verschlüsselten Zustand nicht möglich (S. 132). Auch ändere sich der technische Stand, sodass fortlaufend zu prüfen sei, ob die Verschlüsselung noch zeitgemäß sei. Ebenso werden die Möglichkeiten, eine Strafbarkeit durch Einwilligung der Betroffenen zu umgehen, ausgelotet und auf Praxistauglichkeit hin untersucht.

In Bezug auf § 303a StGB widmet sich *Wicker* unter anderem der Problematik, wie die Löschung einer Sicherungskopie von Daten durch den Cloud-Anbieter (im Regelfall wegen der Erstellung einer neuen Sicherungskopie auf aktuellem Stand) zu bewerten sei. Hiermit verzahnt ist die Frage, ob der Cloud-Anbieter, der technisch bedingt die Daten des Cloud-Nutzers nicht dauerhaft auf einem Server speichert, sondern fortlaufend die Daten auf einen anderen Server kopiert und sodann vom Ursprungsserver löscht, sich gem. § 303a StGB strafbar macht. *Wicker* kommt zu dem Schluss, dass die Löschung anderer Kopien oder durch den Kopiervorgang hergestellter weiterer Originale nicht tatbestandsmäßig sei, solange der Zugang zu den Daten für den Cloud-Nutzer möglich bleibt. Verhindere der Cloud-Anbieter aber den Zugang des Cloud-Nutzers zu den Daten, etwa weil dieser den schuldrechtlichen Zahlungsverpflichtungen nicht nachkomme, sei die Unterdrückensvariante des § 303a StGB gegeben (S. 185). Hierbei sei aber die individuelle Vertragsabrede zu beachten, die ggf. einen Rechtfertigungsgrund statuieren könne.

Im Rahmen des § 353b StGB erkennt *Wicker* ein Strafbarkeitsrisiko durch Nutzung des Cloud Computings von Behörden, sofern keine ausreichende Verschlüsselung genutzt wird. Es ergeben sich viele Parallelen zu § 203 StGB. Anders als dort wird hier aber der Umstand näher beleuchtet, dass oftmals auf Seiten des Cloud-Nutzers die Positionen des Sachbearbeiters, der die Daten speichert, des Administrators, der Kenntnis von der jeweiligen IT-Infrastruktur hat und des Behördenleiters auseinanderfallen. Hierdurch kann die Situation gegeben sein, dass der Sachbearbeiter durch die Speicherung von Daten in der Cloud zwar objektiv tatbestandlich handelt, subjektiv aber nicht die notwendige Kenntnis in seiner Person gegeben ist (S. 215), beim Administrator verhielte es sich umgekehrt. *Wicker* prüft hier eine mögliche Zurechnung und verweist auf die Anwendung der allgemeinen Regelungen des § 25 StGB.

In strafprozessualer Hinsicht verfährt *Wicker* in ähnlicher Weise wie bei der Ermittlung materiell-rechtlicher Strafbarkeitsrisiken. Sie stellt zunächst allgemeine Grundlagen voran, um sodann mögliche Eingriffsermächtigungen zur Datenerhebung in der Cloud zu identifizieren und diese vor deren Tauglichkeit zum Umgang mit Cloud Computing zu untersuchen. Auch hier sollen nur einige wenige Punkte der umfangreichen Untersuchung dargestellt werden.

So geht die *Autorin* in Bezug auf eine mögliche Durchsuchung der Cloud gem. § 102 StPO darauf ein, in wessen Gewahrsam die dort gespeicherten Daten stehen. Nach *Wicker* seien die Server zwar im Gewahrsam des Cloud-Anbieters, durch die mietvertragliche Einordnung des Cloud Computing-Vertrages gelte dies aber nicht für die durch den Vertrag zum Gebrauch überlassenen Ressourcen. Diese seien dem Cloud-Nutzer zugesprochen und ihm durch den jeweiligen Nutzeraccount samt Kennwort auch zuzuordnen, sodass insoweit der Gewahrsam des Cloud-Nutzers begründet sei

(S. 336-341). Dies ist ein innovativer Ansatz, der mit Blick auf die technische Entwicklung und die zivilrechtliche Einordnung dogmatisch fundiert eine der Realität angemessene Lösung bietet.

Sollte der jeweilige Server sich im Ausland befinden, sieht *Wicker* keine Hindernisse, den jeweiligen Cloud-Speicherplatz gem. der §§ 102, 110 Abs. 3 StPO zu durchsuchen. Ein willkürlicher Zugriff inländischer Ermittlungspersonen auf das Ausland sei hier nicht anzunehmen (S. 356). Anders als beim IT-Outsourcing, in dessen Rahmen die Verortung der Server im Ausland bekannt sei, könne diese Kenntnis den Beamten beim Cloud Computing gerade nicht unterstellt werden. Wo sich die Daten befänden, sei oftmals nicht einmal dem Cloud-Anbieter bekannt. Daher sei eine Verortung im Inland nicht ausgeschlossen, ein willkürlicher Zugriff auf das Ausland somit nicht gegeben. Eine solche Ansicht überzeugt wenig. Zwar ist zuzugeben, dass der Praxis hier mit den bisherigen Regeln Grenzen gesetzt sind. Sollte der Ort des jeweiligen Servers tatsächlich ermittelt werden können, ist der Weg über die traditionelle Rechtshilfe meist dermaßen lang, dass die Daten zu dem Zeitpunkt der ersuchten Ermittlungshandlung bereits wieder an einen anderen Server übertragen oder schlicht gelöscht sind. Es ist *Wicker* zuzugeben, dass diese Lösung vor dem Hintergrund der technischen Entwicklung nicht überzeugen kann. Eine recht künstlich wirkende Unwissenheit der Beamten zu postulieren und hierdurch völkerrechtliche Grundsätze auszuhebeln, kann aber dogmatisch auch nicht überzeugen.

Im Übrigen ist die strafprozessuale Analyse ebenso wie die materiell-strafrechtliche detailliert, erschöpfend und argumentativ überzeugend. Die Zusammenfassung zum Schluss bietet zugleich einen aussagekräftigen Überblick und Leitlinien für die weitere Entwicklung. *Wicker* gelangt zu dem Schluss, dass sich unser Strafrechtsregime im Großen und Ganzen gegenüber der neuen Entwicklung des Cloud Computings als robust und sachgerecht darstellt. Sie weist jedoch auf die gefundenen Ergebnisse hin und plädiert für gezielte Korrekturen in einzelnen Bereichen.

Alles in allem ist *Wicker* mit dem Werk eine umfassende Untersuchung zum Thema Cloud Computing und Strafrecht gelungen. Es setzt sich sowohl mit den technischen Grundlagen als auch mit der juristischen Dogmatik auseinander. Dabei ist es gleichermaßen als Beitrag zur wissenschaftlichen Diskussion und als Nachschlagewerk für den juristischen Praktiker geeignet und daher vollumfänglich zu empfehlen.

Dr. Markus Mavany, Trier