Daniel Müller: Cloud Computing. Strafrechtlicher Schutz privater und geschäftlicher Nutzerdaten vor Innentäter-Angriffen de lege lata und de lege ferenda

von Prof. Dr. Anja Schiemann

2020, Duncker & Humblot, ISBN: 978-3-428-15747-1, S. 475, Euro 119,90.

Während es zu strafprozessualen Ermittlungsmöglichkeiten in der Cloud bereits zahlreiche Dissertationen gibt, haben Monografien, die sich mit materiell-rechtlichen Fragen rund um das Cloud Computing beschäftigen, Seltenheitswert. *Müller* stößt mit seiner Dissertation in diese Lücke und legt den Fokus auf eine ganz spezielle Fragestellung, nämlich wie weit der strafrechtliche Schutz privater und geschäftlicher Daten von Angriffen sog. Innentäter reicht. Während das Interesse von Cloudnutzern an der Vertraulichkeit, Unversehrtheit und Erreichbarkeit ihrer in die Cloud ausgelagerten Daten vor Angriffen externer Täter strafrechtlich umfassend geschützt werde, sei äußerst unklar, ob dies auch bei Angriffsformen der Innentäter der Fall sei (S. 27).

Die Dissertation entstand im Rahmen der Mitarbeit an dem Forschungsprojekt „Sicheres Cloud Computing" im Förderzeitraum von 2015-2018. Neben der rechtswissenschaftlichen Disziplin, waren auch Informatiker, Wirtschaftsinformatiker und zahlreiche Unternehmen beteiligt (S. 28).

Müller führt zunächst in die technischen und organisatorischen Besonderheiten des Cloud Computing ein, um in einem zweiten Schritt die Tätergruppe der Innentäter, ihre Tatmotive sowie ihre möglichen Angriffshandlungen vorzustellen. Im Fokus steht dabei der Schutz der Inhaltsdaten. Vor diesem Hintergrund wird in den darauffolgenden Kapiteln untersucht, inwieweit die im Strafgesetzbuch normierten Tatbestände geeignet sind, die Cloud-Nutzer vor einer unbefugten Verschaffung, Kenntnisnahme und Weitergabe ihrer Inhaltsdaten durch Innentäter beim Cloud Computing zu schützen. Darüber hinaus werden auch Vorschriften im Nebenstrafrecht sowie Bußgeldvorschriften der DSGVO, des BDSG, des UWG und TGK beleuchtet. Danach wird auch der strafrechtliche Schutz der Nutzerdaten im Hinblick auf die Manipulation und Beeinträchtigung der Erreichbarkeit ihrer Inhaltsdaten durch Innentäter untersucht. Im Anschluss daran wird der Frage nachgegangen inwieweit strafbare Handlungen der Innentäter überhaupt dem Geltungsbereich des deutschen Strafrechts unterliegen, sofern es sich um grenzüberschreitende Angriffe handelt. Abschließend wird aufgrund der gewonnenen Ergebnisse geklärt, ob Regelungslücken bestehen und wie ggf. rechtliche Anpassungen de lege ferenda auszusehen hätten.

Müller legt eine dezidierte Prüfung sämtlicher in Betracht kommender Normen des Straf- und Ordnungswidrigkeitenrechts vor, wobei nicht nur die kritische Auseinandersetzung mit Schwachstellen, sondern auch der fundierte, sehr große Fußnotenapparat überzeugt.

Nach Auffassung des Verfassers resultieren die Schutzlücken primär daraus, dass die Strafvorschriften der §§ 202a ff. StGB eine fehlende Zugriffsbefugnis und die Überwindung einer zum Tatzeitpunkt wirksamen Sicherheitsmaßnahme fordern. Ein Privilegienmissbrauch der Administrationen sei gerade nicht strafbar, da sie zum einen zugriffsberechtigt seien und es zum anderen bei ihren Angriffshandlungen an einer Überwindung der Sicherheitsvorkehrungen fehle.

Allerdings komme zumindest dann eine Strafbarkeit oder Ordnungswidrigkeit in Betracht, sofern sich die Tat des Innentäters auf Geschäfts- und Betriebsgeheimnisse oder personenbezogene Daten bezöge. Hier stünde eine Verwirklichung der §§ 17 UWG, 42 BDSG und Art. 83 DSGVO im Raum. Allerdings wiesen diese Vorschriften ein erhebliches Vollzugsdefizit aus, so dass sie keine effektive Präventivwirkung entfalten könnten. Unklar sei zudem, ob der datenschutzverstoßende Innentäter überhaupt tauglicher Normadressat des Art. 83 DSGVO sei.

Die Schutzlücke werde durch die Straftatbestände der Verletzung des Fernmeldegeheimnisses gem. § 206 Abs. 1 StGB und der Verletzung und Verwertung von Privatgeheimnissen nach §§ 203 Abs. 4, 204 Abs. 1 StGB nicht hinreichend geschlossen, da diese nur in wenigen, ganz bestimmten Fallkonstellationen griffen.

Aufgrund dieser Strafbarkeitslücken überlegt *Müller,* ob eine Ergänzung der Tätergruppe des § 203 Abs. 1 StGB um „Angehörige von IT-Dienstleistungsunternehmen" sinnvoll wäre, um diese Lücken zu schließen. Er kommt aber zu dem Ergebnis, dass es kaum möglich sei, den Täterkreis so hinreichend bestimmt zu formulieren, dass nur solche Tätigkeiten eines IT-Dienstleistungsunternehmen in den Anwendungsbereich der Strafnorm fielen, die sich nach ihrer ratio legis gerade auf den Geheimnisschutzbereich bezögen und keine anderen Berufstätigkeitsfelder beträfen, die keinen Kontakt mit schützenswerten geheimen Daten erforderten.

Der Verfasser spricht sich vielmehr für die Schaffung eines neuen Straftatbestands aus und möchte in § 202d StGB-E die Datenuntreue gesetzlich normieren (S. 405). Er möchte den Rechtsgedanken der Untreue gem. § 266 StGB auf das Cloud Computing übertragen. Die Erweiterung des strafrechtlichen Schutzes um einen Straftatbestand der Datenuntreue stehe der ultima ratio Funktion des Strafrechts nicht entgegen. Weder sei eine rein technische

Lösung zum Schutz des Verfügungsrechts der Cloud-Nutzer ausreichend, noch seien die bisher existierenden Bußgeldsanktionen ausreichend, da nur wenige Adressaten zur Verantwortung gezogen werden könnten. Daher bedürfe es aus spezial- und generalpräventiven Gründen einer verhaltenssteuernden Regelung im Strafrecht, um die Inhaltsdaten der Cloud-Nutzer angemessen vor den potentiellen Gefahren der Innentäter zu schützen. Auch stünde der Ergänzung des strafrechtlichen Schutzes durch Einführung eines § 202d StGB nicht Art. 2 CCC entgegen. Dieser sei aber bei einer Ausformulierung zu berücksichtigen, so dass *Müller* schließlich zu folgendem de lege ferenda Vorschlag kommt:

„*202d StGB Datenuntreue*

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, für ihn bestimmte, nicht allgemein zugängliche Daten (§ 202a Abs. 4), die ihm als Inhaber oder Beschäftigtem eines Unternehmens, das geschäftsmäßig fremde Daten mit der Maßgabe einer besonderen Sicherung in einem vernetzten Computersystem speichert oder verarbeitet, anvertraut wurde, sich oder einem anderen unbefugt verschafft, verkauft, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Absatz 1 gilt auch für Personen, die mit der Nutzung und Verwaltung der in Absatz 1 bezeichneten IT-Dienstleistungen aufgrund ihres Beschäftigungsverhältnisses zum Dienstleistungsnutzer betraut wurden.

(3) In besonders schweren Fällen des Absatzes 1 und 2 ist die Strafe Freiheitsstrafe bis zu drei Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

> *1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach Absatz 1 verbunden hat oder*
>
> *2. Daten einer großen Zahl von Personen sich oder einem anderen verschafft, verkauft, verbreitet oder sonst zugänglich macht.“ (S. 403).*

Darüber hinaus sieht *Müller* einen gewissen Änderungsbedarf bei § 202a StGB. Er möchte einen dogmatischen Widerspruch zu § 202c StGB auflösen und in § 202a StGB-E die versuchte Tatbegehung miterfassen (S. 410). Um einen vollumfassenden Schutz der Datenvertraulichkeit vor sämtlichen Erscheinungsformen einer Side-Channel-Attacke zu gewährleisten, schlägt der Verfasser zudem vor, die zweite Tatbestandsalternative des § 202b StGB technikneutraler zu formulieren und „durch die Analyse des Systemverhaltens“ einzufügen (S. 410). Darüber hinaus soll bei § 202c StGB mit Absatz 3 ein neuer Qualifikationstatbestand für gewerbs- und bandenmäßige Begehung ergänzt werden, um für einen effektiven und abschreckenden strafrechtlichen Schutz zu sorgen (S. 411). Des Weiteren spricht sich *Müller* ebenfalls bei der Datenhehlerei für die Einfügung eines entsprechenden Qualifikationstatbestands aus (S. 412). Das Strafantragserfordernis nach § 205 StGB sollte um den neu normierten Straftatbestand der Datenuntreue ergänzt werden (S. 413).

Im Hinblick auf den Schutz der Integrität und Verfügbarkeit der Nutzerdaten schlägt der Verfasser eine Änderung des § 303a StGB vor. Gewisse Schutzlücken im Bereich der Datenveränderung ergäben sich in Fällen banden- oder gewerbsmäßiger Begehung. Außerdem fände sich kein Regelbeispiel für den Fall, dass durch den Innentäter-Angriff ein materieller Schaden von besonders großem Ausmaß beim Cloud-Nutzer eingetreten sei. Des Weiteren solle ein Regelbeispiel für die Konstellation greifen, wenn durch die Straftat des Innentäters die Datenverfügungsbefugnis einer großen Zahl von Privatnutzern verletzt werde (S. 414 f.).

Änderungsbedarf zeigt *Müller* ebenfalls bei der Computersabotage gem. § 303b StGB auf. So sollten die in Abs. 4 benannten Strafzumessungsgründe nicht nur auf die Cloud nutzenden Unternehmen und Behörden, sondern auch auf Privatpersonen anwendbar sein. Um darüber hinaus Fallkonstellationen des Cloud War und der DDOS-Angriffe, die unter Verwendung privater IT-Systeme durchgeführt werden, strafrechtlich besser ahnden zu können, sollte das Regelbeispiel zudem durch das Merkmal der Beeinträchtigung einer großen Anzahl von Datenverarbeitungsvorgängen informatorischer Systeme ergänzt werden (S. 415 f.).

Um darüber hinaus strafanwendungsrechtliche Lücken zu schließen, schlägt der Verfasser eine Ergänzung des § 5 StGB (Auslandstaten mit besonderem Inlandsbezug) vor. Gem. § 5 Nr. 7 lit. a StGB soll deutsches Strafrecht unabhängig vom Recht des Tatortes für folgende Taten, die im Ausland begangen werden, gelten: „Straftaten nach den §§ 202a bis 204 und § 206 sowie nach den §§ 274 Abs. 1 Nr. 2, Abs. 2, 303a, 303b und § 42 BDSG, wenn der Täter zur Zeit der Tat Deutscher ist oder wenn sich die Tat gegen eine Person richtet, die zur Zeit der Tat ihren Wohnsitz oder gewöhnlichen Aufenthalt in Deutschland hat, sofern sich die Tat auf eine Datenverarbeitung bezieht, die in Zusammenhang damit steht, den betroffenen Personen im Inland Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von den betroffenen Personen eine Zahlung zu leisten ist“ (S. 419).

Durch die umfangreichen de lege ferenda Vorschläge bietet die Dissertation breiten Raum für die kriminalpolitische Diskussion, ob und wie der strafrechtliche Schutz privater und geschäftlicher Daten vor Innentäter-Angriffen ausgestaltet werden kann. Der Verfasser hat ausführlich dargelegt, wo die Schutzlücken im geltenden materiellen Strafrecht zu finden sind. Die de lege ferenda Vorschläge sind moderat und liegen zum einen in einer leichten Anpassung bestehender Regeln, insbesondere um die Erweiterung von Regelbeispielen, aber auch in einem neuen eigenständigen Straftatbestand der Datenuntreue. Die Herleitung überzeugt und auch dem ultima ratio Gedanken wird Rechnung getragen und die Eingriffe so minimalinvasiv wie möglich ausgestaltet. Von daher bleibt

zu hoffen, dass die Dissertation einen großen Leserkreis findet und der kriminalpolitische Diskurs im Hinblick auf die Überarbeitung des sog. Computerstrafrechts insgesamt weiter an Fahrt aufnimmt.