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

Andreas Grözinger, Die Überwachung von Cloud-Storage, Eine Untersuchung der strafprozessualen Möglichkeiten zur heimlichen Überwachung von Cloud-Storage vor und nach dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, Nomos Verlagsgesellschaft, Baden-Baden, 2018, 347 S., € 89.

Die Arbeit von *Grözinger* wurde im Wintersemester 2017/2018 an der Universität zu Köln als Dissertation angenommen, die gedruckte Fassung befindet sich inhaltlich auf dem Stand von August 2018. Die Arbeit ist in insgesamt sieben Abschnitte gegliedert: Nach einer kurzen Einleitung (§ 1) erläutert *Grözinger* die begrifflichen und technischen Grundlagen des Cloud-Storage sowie die Vorteile heimlicher Ermittlungsmaßnahmen (§ 2). Er untersucht im folgenden Kapitel die verfassungsrechtlichen Grundlagen (§ 3) und beschreibt sodann die gesetzlichen Eingriffsnormen der Strafprozessordnung vor der Reform durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.8.2017[1] (§ 4). Im Anschluss erläutert *Grözinger* die prozessualen Rechtsfolgen im Falle eines unzulässigen Eingriffs (§ 5). Darauf wird im nächsten Kapitel die Rechtslage nach der vorgenannten Reform der Strafprozessordnung dargestellt und die nunmehr eingeführten Rechtsgrundlagen werden dahingehend überprüft, ob sie als Ermächtigungsgrundlage für Strafverfolgungsbehörden zum heimlichen Zugriff auf Cloud-Storage dienen können (§ 6). Im letzten Kapitel fasst der *Autor* die Ergebnisse seiner Arbeit zusammen (§ 7).

Grözinger beschreibt zunächst im zweiten Abschnitt (§ 2) den Begriff des Cloud-Storage und legt seiner Arbeit die Definition der US-amerikanischen Standardisierungsstelle National Institute of Standards and Technology (NIST) zugrunde (S. 32 f.). Demnach ist Cloud-Storage als ein Modell zu verstehen, „das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Server-Provider-Interaktion zur Verfügung gestellt werden können“ (S. 32). Im Anschluss erläutert *Grözinger* die technischen Grundlagen des Cloud-Storage und schließlich die praktischen Möglichkeiten zur Überwachung einer Cloud (S. 37 ff.). Dabei geht er auch auf die Problematik des Speicherorts der Daten ein, die gerade beim Cloud-Storage besonders relevant ist, da die Server, auf denen die Daten gespeichert werden, im Ausland stehen können. Ein Zugriff auf Cloud-Storage durch deutsche Ermittlungsbehörden auf Grundlage strafprozessualer Ermächtigungsnormen kann nur erfolgen, wenn sich die Server in der Bundesrepublik Deutschland befinden, ansonsten kann das Souveränitätsrecht des Staates beeinträchtigt sein, in dessen Staatsgebiet die Server sich befinden (S. 53 f.).[2]

Im dritten Abschnitt (§ 3) befasst sich *Grözinger* mit den verfassungsrechtlichen Grundlagen heimlicher Zugriffe auf Cloud-Storage. Der *Autor* unterteilt die Nutzung von Cloud-Storage anhand der Anzahl der jeweiligen Nutzer in zwei Fallgruppen: Demnach ist zu unterscheiden, ob Cloud-Storage durch eine Person („klassisches“ Cloud-Storage) oder mehrere Personen (telekommunikatives Cloud-Storage) genutzt wird. Anschließend prüft *Grözinger*, welche Grundrechte auf die Fallgruppen Anwendung finden (S. 125 ff.). Er kommt zu dem Ergebnis, dass die Nutzung von Cloud-Storage durch eine Person grundsätzlich nicht durch Art. 10 GG geschützt ist. Diese Konstellation unterfällt vielmehr dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) und wird durch dieses geschützt; auch das Recht auf informationelle Selbstbestimmung ist bei der Nutzung durch eine Person nur ausnahmsweise anwendbar (S. 140). *Grözinger* erläutert im Folgenden ausführlich Schutz- sowie Anwendungsbereich des neuen IT-Grundrechts und wendet es konsequent auf Cloud-Storage durch eine Einzelperson an. Bei der Verwendung von Cloud-Storage durch mehrere Personen, dem telekommunikativen Cloud-Storage, greift das Telekommunikationsgrundrecht, sodass Art. 10 GG in diesem Fall einschlägig ist.

Im vierten Abschnitt (§ 4) prüft der *Verfasser*, ob und inwieweit die – nunmehr – alten Ermächtigungen der Strafprozessordnung einen heimlichen Zugriff auf Cloud-Storage rechtfertigen konnten. Er untersucht dabei insbesondere die Norm des § 100a StPO a.F. Zunächst befasst er sich mit dem Telekommunikationsbegriff und stellt die bestehenden Ansichten (technische und materielle Auslegung des Begriffs) dar. Im Anschluss prüft er, inwieweit es sich bei der Nutzung von Cloud-Storage um Telekommunikation handelt (S. 188 ff.). Er untersucht dies für beide von ihm dargestellten Telekommunikationsbegriffe, die jeweils unterschiedliche Strömungen enthalten, und lehnt eine rein technikorientierte Auslegung des Telekommunikationsbegriffs ab (S. 210). Er legt seiner Arbeit einen materiellen Telekommunikationsbegriff zugrunde, wobei er sich der Strömung anschließt, nach der der strafprozessuale Telekommunikationsbegriff dem grundrechtlichen Telekommunikationsbegriff des Art. 10 Abs. 1 Var. 3 GG entspricht (S. 215).[3] *Grözinger* kommt zu dem Ergebnis, dass Cloud-Storage dann Telekommunikation i.S.v. § 100a StPO a.F. darstellt, wenn Cloud-Storage durch mehrere Personen betrieben wird (telekommunikatives Cloud-

[1] BGBl. 2017 I, S. 3202; siehe zu dieser Gesetzesänderung *Singelnstein/Derin*, NJW 2017, 2646; *Niedernhuber*, JA 2018, 169; siehe auch *Graf*, in: Graf (Hrsg.), Beck’scher Online-Kommentar, Strafprozessordnung, Stand: 1.4.2019, § 100a Rn. 14 f.; insbesondere zur neu eingeführten Online-Durchsuchung siehe *Soiné*, NStZ 2018, 497; krit. zur Gesetzesänderung *Beukelmann*, NJW-Spezial 2017, 440; *Roggan*, StV 2017, 821.

[2] Zum grenzüberschreitenden Zugriff auf Cloud-Daten siehe auch *Burchard*, ZIS 2018, 190; *ders.*, ZIS 2018, 249.

[3] So etwa auch *Neuhöfer*, Der Zugriff auf serverbasiert gespeicherte E-Mails beim Provider, 2011, S. 60; vgl. zu einem genuinen strafprozessualen Telekommunikationsbegriff etwa *Gercke*, GA 2012, 474; *ders.*, StraFo 2003, 76 (78); *Ihwas*, Strafverfolgung in Sozialen Netzwerken, 2014, S. 206.

Storage; S. 215). Im Falle der Nutzung von Cloud-Storage durch nur eine Person handelt es sich dementsprechend nicht um Telekommunikation i.S.d. Vorschrift und § 100a StPO a.F., der seinem Wortlaut nach ausdrücklich Telekommunikation durch den Betroffenen verlangt, stellt keine taugliche Ermächtigungsgrundlage für eine entsprechende Ermittlungsmaßnahme dar.

Im Folgenden untersucht der *Autor*, wann § 100a StPO a.F. eine taugliche Ermächtigungsgrundlage für den Zugriff im Falle von telekommunikativem Cloud-Storage darstellt (S. 216 ff.). Dies ist jedenfalls dann zu bejahen, wenn die Daten auf dem Übertragungsweg in die Cloud überwacht oder die Daten zeitlich nach dem Erlass der Überwachungsanordnung in der Cloud gespeichert werden (S. 248). Soweit Daten vor dem Erlass der Anordnung bereits in der Cloud gespeichert worden sind, können diese nicht mehr im Sinne der Norm des § 100a StPO a.F. „überwacht" werden, sodass eine Anwendbarkeit der Vorschrift insoweit nicht in Betracht kommt.

In der gebotenen Kürze untersucht *Grözinger* sodann weitere strafprozessuale Ermächtigungsgrundlagen und kommt zu dem Ergebnis, dass keine weitere Ermächtigung geeignet ist, eine heimliche Überwachung von Cloud-Storage zu rechtfertigen (S. 253). Im nächsten Abschnitt (§ 5) erläutert der *Verfasser* die prozessualen Rechtsfolgen im Falle einer rechtswidrigen Überwachung von Cloud-Storage (S. 256 ff.).

Der sechste Abschnitt (§ 6) befasst sich mit der Zulässigkeit der Überwachung von Cloud-Storage nach der Reform der Strafprozessordnung im Jahr 2017 (S. 265 ff.). *Grözinger* beschreibt zunächst die neuen Regelungen und wendet diese auf die Überwachung von Cloud-Storage an. Dieses Kapitel ist das Kernstück der Arbeit und beleuchtet in der gebotenen Tiefe die neuen strafprozessualen Ermächtigungen. *Grözinger* untersucht zunächst die Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 S. 2 StPO) und die „kleine Systemüberwachung"[4] (§ 100a Abs. 1 S. 3 StPO).[5] Im Anschluss widmet er sich der Online-Durchsuchung (§ 100b StPO) und kommt zu dem Ergebnis, dass die neuen Normen die Strafverfolgungsbehörden zwar zu einer annähernd lückenlosen Überwachung von Cloud-Storage ermächtigen (S. 288), diese Ermächtigungsnormen allerdings verfassungswidrig sind (S. 316):

Hinsichtlich der Quellen-Telekommunikationsüberwachung arbeitet der *Autor* heraus, dass diese deutlich tiefer in das Telekommunikationsgeheimnis eingreift, als es bei der herkömmlichen Telekommunikationsüberwachung nach § 100a Abs. 1 S. 1 StPO der Fall ist. Daher ist die durch den Gesetzgeber erfolgte Übernahme des Straftatenkatalogs des § 100a Abs. 2 StPO, der maßgeblich auf eine Telekommunikationsüberwachung nach § 100a Abs. 1 S. 1 StPO zugeschnitten ist, für die Quellen-Telekommunikationsüberwachung unzulässig (S. 291) und die Norm insbesondere deswegen verfassungswidrig. Die Vorschrift des § 100a Abs. 1 S. 3 StPO, die die „kleine Systemüberwachung" regelt, ist ebenfalls verfassungswidrig, da auch auf sie der Katalog der Norm des § 100a Abs. 2 StPO angewendet wird (S. 299). Denn die „kleine Systemüberwachung" stellt einen Eingriff in das IT-Grundrecht dar und der Katalog des § 100a Abs. 2 StPO widerspricht den vom Bundesverfassungsgericht aufgestellten Maßstäben für die Zulässigkeit heimlicher Eingriffe in das IT-Grundrecht. Ein solcher Eingriff darf nur zur Verfolgung von Straftaten erfolgen, die ein überragend wichtiges Rechtsgut schützen. Dies ist nicht bei allen in § 100a Abs. 2 StPO genannten Delikten der Fall (S. 300). Zudem greift – auch – die „kleine Systemüberwachung" deutlich tiefer in die Rechte des Betroffenen ein als die herkömmliche Telekommunikationsüberwachung.

Schließlich prüft *Grözinger* die Online-Durchsuchung nach der Norm des § 100b StPO und kommt hier ebenso zu dem Ergebnis, dass diese verfassungswidrig ist (S. 309). Die wortlautgleiche Übernahme des Straftatenkatalogs des § 100c Abs. 2 StPO (akustische Wohnraumüberwachung) in § 100b Abs. 2 StPO ist unzulässig (S. 305). Die Norm muss einen Eingriff in das IT-Grundrecht rechtfertigen, was nur zum Schutz überragend wichtiger Rechtsgüter zulässig ist. Allerdings schützt nicht jedes im Straftatenkatalog des § 100b Abs. 2 StPO genannte Delikt ein solches Rechtsgut (S. 306).

Grözinger fasst sodann den gesetzgeberischen Handlungsbedarf zusammen (S. 317 ff.) und unterbreitet konkrete Vorschläge, wie die Ermächtigungsnormen zukünftig formuliert sein könnten.

Insgesamt handelt die Arbeit von einem hochaktuellen Thema, das aufgrund der fortschreitenden Technisierung stetig mehr Relevanz bekommt. Cloud-Dienste erfreuen sich bei den Internetnutzern immer größerer Beliebtheit und werden dementsprechend immer häufiger genutzt. Oft werden diese Cloud-Dienste auch kostenfrei zur Verfügung gestellt, was ihre Verbreitung erhöht. Damit einhergehend steigt gleichermaßen die Bedeutung von Cloud-Storage-Diensten im Zusammenhang mit strafrechtlichen Ermittlungen. Die Arbeit erläutert – auch für den technisch nicht versierten Leser – in klaren Worten die technischen Grundlagen des Cloud-Storage und bietet einen umfassenden Überblick über die alten und neuen rechtlichen Ermächtigungsnormen. Dabei erläutert der *Autor* ebenso das zugehörige Verfassungsrecht in der gebotenen Tiefe; besonders hervorzuheben sind hier die Ausführungen zu dem verhältnismäßig jungen IT-Grundrecht. Die große Leistung der Arbeit liegt in der kenntnisreichen Darstellung der komplexen Schnittstelle zwischen Freiheitsrechten und Eingriffsbefugnissen, wobei es *Grözinger* gelingt, dem Leser einen abschließenden Überblick hinsichtlich der aktuellen rechtlichen Probleme in diesem Bereich zu geben. Es handelt sich im Ergebnis um eine – zu Recht – umfangreiche Arbeit, die keine Fragen offenlässt und jedem zu empfehlen ist, der in diesem Bereich tätig ist. Darüber hinaus wurden im Jahr 2018 bereits mehrere Verfassungsbe-

[4] Eine Maßnahme nach § 100a Abs. 1 S. 3 StPO stellt einen tieferen Eingriff als eine Telekommunikationsüberwachung dar, da die Vorschrift es auch gestattet, auf Kommunikation zuzugreifen, die auf dem Endgerät des Betroffenen nach Abschluss des Übertragungsvorgangs gespeichert wird (S. 297).

[5] § 100a Abs. 1 S. 1 StPO a.F. entspricht § 100a Abs. 1 S. 1 StPO n.F., sodass *Grözinger* hierzu auf seine vorangehenden Ausführungen verweist.

schwerden gegen die neuen Ermächtigungsnormen beim Bundesverfassungsgericht eingereicht.[6] *Grözinger* wird daher durch eine Vielzahl von Vertretern in seiner Ansicht gestützt, dass diese Vorschriften verfassungswidrig sind.

Rechtsanwalt Dr. Saleh R. Ihwas, Mainz

[6] Vgl. hierzu etwa *Greis*, golem v. 7.8.2018, abrufbar unter https://www.golem.de/news/verfassungsbeschwerde-digitalcourage-klagt-gegen-staatstrojaner-1808-135878.html (20.5.2019); *Sehl*, LTO v. 20.8.2019, abrufbar unter https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-staatstrojaner-fdp-anwalt-interview-online-durchsuchung/ (20.5.2019).