



**University of
Zurich**^{UZH}

**Zurich Open Repository and
Archive**

University of Zurich
University Library
Strickhofstrasse 39
CH-8057 Zurich
www.zora.uzh.ch

Year: 2008

**Rezension von: Marc Störing, Strafprozessuale Zugriffsmöglichkeiten auf
E-Mail-Kommunikation (Logos Verlag, Berlin 2007)**

Schlegel, Stephan

Posted at the Zurich Open Repository and Archive, University of Zurich
ZORA URL: <https://doi.org/10.5167/uzh-13161>
Journal Article

Originally published at:

Schlegel, Stephan (2008). Rezension von: Marc Störing, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation (Logos Verlag, Berlin 2007). *Höchstrichterliche Rechtsprechung im Strafrecht (HRRS)*, 9(1):213-214.

einschätzen an einem solchen Bewusstsein. Viele würden gar nicht wissen, was die BaFin sei und was diese tue.

5. In seinem Fazit stellt *Hienzsch* fest, dass es dem gesetzlichen Insiderhandelsverbot in Deutschland kaum gelungen sei, Anlegervertrauen zu fördern (S. 195). Verantwortlich sei hierfür einerseits die schwierige Durchsetzbarkeit von Insidernormen sowie andererseits die Tatsache, dass ein Insiderhandelsverbot für sich genommen nicht geeignet sei Vertrauen in den Kapitalmarkt herzustellen. Die Schwierigkeiten bei der Durchsetzbarkeit können nicht durch eine materielle Ausdehnung der Strafbarkeit aufgefangen werden, wie dies bereits durch Schaffung von Bußgeldvorschriften bei nur leichtfertigem Insiderhandel geschehen sei (S. 196). Begrüßenswert sei im Gegensatz dazu die Einführung der Ad-hoc-Mitteilungspflicht, die geeignet sei durch Markttransparenz das Vertrauen der Anleger in den Kapitalmarkt zu stärken. Gerade durch die Schaffung eines wirksamen zivilrechtlichen Anlegerschutzes könne ein bedeutender Schritt in Richtung einer gesicherten Funktionsfähigkeit des Kapitalmarktes getan werden (S. 197).

III. *Hienzsch* ist es mit seiner Untersuchung gelungen einen spannenden Einblick in die Verfolgungstätigkeit von BaFin und Staatsanwaltschaften bei Insiderdelikten zu geben. Interessant ist insbesondere die Selbsteinschätzung der Mitarbeiter der Verfolgungsorgane, wie sie durch die Expertenbefragung deutlich wird. Dass *Hienzsch* hierbei nur eine geringe Anzahl von Probanden befragen konnte (15 zur ersten und 10 zur zweiten Forschungsfrage) ist bedauerlich, aber auch nachvollziehbar, da es sich um einen langen und nur aufwendig auszuwertenden Fragenkatalog handelt. Zudem kann dem Verf. nicht angelastet werden, dass jedenfalls bei der BaFin ohnehin nur eine kleine Gruppe von potenziellen Experten existiert, die sich schwerpunktmäßig mit Insiderhandel beschäftigen. Die von *Hienzsch* festgestellten Verfolgungsdefizite bei den Staatsanwaltschaften in materieller und personeller Hinsicht dürften sich ganz grundsätzlich bei der Strafverfolgung von Wirtschaftsstraftaten zeigen, da es hier beinahe immer erforderlich ist komplizierte wirtschaftliche Zusammenhänge zu durchschauen, um die Sachverhalte auf ihre strafrechtliche Relevanz überprüfen zu können. Das wiederum ändert freilich nichts an der Notwendigkeit von *Hienzsch* Forderung Schwerpunktstaatsanwaltschaften einzurichten, wobei zugegebenermaßen in der rechtspolitischen Diskussion auch sonst für fast jedes Delikt entsprechende Forderungen schnell aufkommen.

Akad. Rätin a. Z. **Silke Noltensmeier**, Universität Erlangen-Nürnberg

Marc Störing: Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation; Logos Verlag, Berlin 2007, 293 S., 40,50 EUR, ISBN 978-3-8325-160-8.

„An der E-Mail kommt fast niemand mehr vorbei.“ so lautete die Schlagzeile eines Artikels in der Welt vom 14. Mai 2007. Zwanzig Jahre nach der ersten „deutschen E-Mail“ im Jahre 1984 nutzen 2006 fast zwei Drittel der

16- bis 74-Jährigen in Deutschland dieses Kommunikationsmittel – mit steigender Tendenz. Als Quelle für die Informationsgewinnung in Strafverfahren ist die E-Mail schon seit mehreren Jahren auch in das Blickfeld der Strafverfolgungsbehörden gelangt. Angefangen mit der so genannten Mailbox-Entscheidung des Ermittlungsrichters des BGH aus dem Jahr 1995 (vgl. NStZ 1997, 247), war der strafprozessuale Zugriff auf diese Form der Kommunikation immer wieder Gegenstand höchstrichterlicher Entscheidungen und kontroverser Auseinandersetzungen in der Literatur. *Marc Störing* widmet sich in seiner von *Klaus Bernsmann* (Bochum) betreuten Dissertation umfassend den mit dem Zugriff auf E-Mail-Kommunikation zusammenhängenden Rechtsfragen. Ausgeklammert bleiben Fragen der Sicherstellungs- sowie der Beweisverwertungsverbote (S. 3).

Die Arbeit untergliedert sich in vier Teile. Im ersten Teil (B.) stellt *Störing* die technischen Grundlage der E-Mail-Kommunikation und die mit ihr zusammenhängenden verfassungsrechtlichen Fragen dar. In den beiden darauf folgenden Teilen untersucht er die einzelnen Zugriffsbefugnisse, d.h. die Beschlagnahmenvorschriften (C.) bzw. die Vorschriften über die Telekommunikationsüberwachung (D.) während er im vierten Teil (D.) seine Erkenntnisse auf die einzelnen Phasen der E-Mail-Kommunikation überträgt.

Auf den Seiten 5 – 24 stellt *Störing* zunächst überblicksartig und leicht verständlich die technischen Grundlagen der E-Mail-Kommunikation und die relevanten Begrifflichkeiten dar. Dies ermöglicht es, sich bei später auftretenden Frage zu einem bestimmten Begriff dessen Bedeutung noch einmal in Erinnerung zu rufen. Auf den folgenden Seiten (24 – 35) zeigt er die verfassungsrechtlichen Grundlagen der E-Mail-Kommunikation auf. Zunächst lehnt er die Rundfunk- und Pressefreiheit nach Art. 5 Abs. 1 S. 2 GG als nicht einschlägig ab, um sich dann der informationellen Selbstbestimmung, Art. 2 Abs. 1 GG, und dem Fernmeldegeheimnis, Art. 10 GG, zuzuwenden, deren Einschlägigkeit er bejaht, während er das Brief- und Postgeheimnis als nicht tangiert ansieht. Leider gerät dieser verfassungsrechtliche Teil etwas knapp, auch wenn Einzelfragen in den weiteren Teilen der Arbeit vertieft werden. Gerade im Hinblick auf Art. 5 Abs. 1 S. 2 GG dürften sich mit der immer stärkeren Durchdringung der Gesellschaft durch die elektronischen Nachrichtenübermittlung in der Zukunft Anwendungsfragen stellen, die jedenfalls mit einem bloßen Verweis auf das jahrhundertalte Vervielfältigungsverfahren des Papierdrucks nicht zu beantworten sein werden.

Daran anschließend thematisiert *Störing* umfassend die im Zusammenhang mit der E-Mail-Kommunikation anfallenden Daten (S. 36 – 51), deren Beweiseignung (S. 51 – 56) und den damit zusammenhängenden Zugriffsmöglichkeiten (S. 56 – 60). Gerade die wenigen Seiten unter dem Titel „Beweisfragen“ (S. 51 ff.) seien allen ans Herz gelegt, die mit der Notwendigkeit des Zugriffs auf E-Mail für die Erkenntnisgewinnung im Strafverfahren argumentieren.

In seinem zweiten Teil (S. 65 – 120) untersucht *Störing* eingehend die Eingriffsgrundlage des § 94 StPO – Sicherstellung von Beweisgegenständen. Dabei prüft er umfas-

send, ob E-Mails isoliert betrachtet als nicht unmittelbar wahrnehmbare elektronische Daten dem Gegenstandsbegriff des § 94 StPO unterfallen und verneint dies mit durchaus überzeugenden Argumenten (S. 80 f.). Als Objekt der Sicherstellung kommen nach seiner Auffassung nur die Datenträger in Betracht (S. 81). Als Folgerung aus dieser Erkenntnis lehnt er (entgegen der Rechtsprechung BVerfGE 113, 29 = HRRS 2005 Nr. 549 und wohl herrschenden Meinung) eine Sicherstellung von Daten durch Kopieren auf Grundlage des § 94 StPO ab. Das Verhältnismäßigkeitsprinzip könne hier nicht herangezogen werden, weil in dieser Vorgehensweise kein *Weniger*, sondern ein *aliud* liege (S. 106 f.). In einer umfassenden Auseinandersetzung kommt der Verfasser zum Schluss, dass § 94 StPO im Hinblick auf die informationelle Selbstbestimmung beim Datenzugriff verfassungswidrig ist (S. 109 ff.). Konsequenterweise mahnt *Störing* daher ein Tätigwerden des Gesetzgebers an (S. 120).

An diese Betrachtungen schliesst sich der dritte Teil der Arbeit unter dem Titel „Telekommunikationsüberwachung § 100a StPO“ an (S. 121–176). Hier geht *Störing* zunächst auf die rechtsgeschichtliche Entwicklung der Telekommunikationsüberwachung in der StPO (S. 121–129), ihre Verbindungen zu anderen Vorschriften (S. 130–135) und die formellen und materiellen Voraussetzungen des § 100a StPO (S. 135–151) ein. Im Rahmen der Verhältnismäßigkeit diskutiert er unter anderem die Eignung der Überwachung unter dem Gesichtspunkt der Kryptologie. Daran anschliessend beschäftigt sich der Verfasser unter dem Titel „Rechtspolitische Betrachtung“ ausführlich mit der praktischen und rechtstatsächlichen Entwicklung der Telekommunikationsüberwachung (S. 151–175). Einen Schwerpunkt bildet darin die Auseinandersetzung mit der Rechtsprechung des BVerfG zum Kernbereich privater Lebensgestaltung (vgl. BVerfGE 109, 279 = HRRS 2004 Nr. 170 und BVerfGE 113, 348 = HRRS 2005 Nr. 718). *Störing* überträgt die Kriterien dieser Rechtsprechung auf die E-Mail-Kommunikation und kritisiert hier überzeugend ihre schwierige Umsetzbarkeit und praktische Wirksamkeit.

Zentraler Abschnitt der Arbeit ist der Teil „Kommunikationsphasen und Zugriffsbefugnisse“ (S. 177–228). In diesem überträgt der Verfasser seine Erkenntnisse aus den vorangegangenen Teilen in einer sehr ausführlichen Auseinandersetzung mit der bis zur Drucklegung (2007) umfassend erhobenen veröffentlichten Rechtsprechung und Literatur. Den überwiegenden Raum des betreffenden Teils der Arbeit nimmt hier die kontrovers geführte Auseinandersetzung um die richtige Rechtsgrundlage für einen Zugriff auf die in der Empfänger-Mailbox bei einem E-Mail-Provider gespeicherten Nachrichten ein, während beispielsweise der Zugriff beim Absender und Empfänger und zwischen Provider und Endnutzer recht kurz behandelt werden. Bisher ist die Frage des Zugriffs

auf beim Provider lagernde E-Mail noch nicht abschließend geklärt. Während beispielsweise das LG Braunschweig in einer Entscheidung aus dem Jahr 2006 (Beschluss vom 12. April 2006 – 6 Qs 88, 97/06) die Beschlagnahmenvorschriften für anwendbar erachtet, lehnt dies das LG Hamburg (Beschluss vom 8.1.2008, Aktenzeichen 619 Qs 1/08), unter Bezugnahme u.a. auch auf die hier besprochene Arbeit, zutreffend ab und hält allein § 100a StPO für einschlägig. Eine abschließende Entscheidung des BVerfG zu dieser Frage steht bisher immer noch aus (vgl. die Anordnung des BVerfG HRRS 2007 Nr. 125 – verlängert durch Beschluss vom 29.11.2007; dazu *Schlegel* HRRS 2007, 44 ff.).

Störing geht zunächst auf die unterschiedlichen Zugriffsmöglichkeiten auf die E-Mail-Kommunikation ein. Dabei erörtert er auch die Frage des heimlichen Zugriffs unter Zuhilfenahme aufgefundener Passwörter, wobei er zutreffend – nunmehr auch verfassungsgerichtlich bestätigt (vgl. BVerfG HRRS 2008 Nr. 160) – Art 13 GG beim Provider als nicht tangiert ansieht (S. 182 ff.). Im Weiteren setzt er sich vertieft und kritisch mit dem insbesondere von *Palm/Roy* (NJW 1996, 1791 ff.) vertretenen sog. Drei-Pasen-Modell auseinander. Nach diesem ist die beim Provider gespeicherte, *aber noch nicht abgerufene* E-Mail in einer Ruheposition (2. Phase) und nicht vom Fernmeldegeheimnis erfasst, während die Übertragungen vom Sender zum E-Mail-Provider und der spätere Abruf durch Art. 10 GG geschützt seien. Überzeugend lehnt er diese Differenzierung ab, weil es im Hinblick auf Art. 10 GG darauf ankommt, ob Dritte – insbesondere der Provider – auf die Kommunikation zugreifen können (S. 197 ff., 209). Sodann widmet er sich dem Problem der *bereits abgerufenen* E-Mails, die (auch) noch beim Anbieter lagern (S. 209 ff.). Soweit sie sich dort befinden, sieht sie der Verfasser mit überzeugender Argumentation als vom Grundrecht des Art. 10 GG geschützt an und will den Zugriff allein über den Weg des § 100a StPO ermöglichen (S. 220 ff.). Im Resümee (S. 229–242) seiner Arbeit geht *Störing* noch überblicksartig u.a. auf die Vorratsdatenspeicherung von Verkehrsdaten ein (S. 236–242), die er als verfassungswidrig ansieht.

Insgesamt bleibt festzuhalten, dass es sich bei der Dissertation von *Störing* um eine gut lesbare Arbeit mit deutlicher Schwerpunktsetzung handelt. Ihre Lektüre sei auch Praktikern ans Herz gelegt, die sich mit Rechtsfragen rund um den strafprozessualen Zugriff auf E-Mail-Kommunikation beschäftigen.

Stephan Schlegel, Wiss. Ass. Universität Zürich
