Sebastian Bauer: Soziale Netzwerke und strafprozessuale Ermittlungen

von Prof. Dr. Anja Schiemann

2018, Duncker & Humblot GmbH, Berlin, ISBN: 978-3-428-15235-3, S. 406, Euro 89,90.

Die Dissertation von *Bauer* wurde 2018 veröffentlicht, der Stand der Literatur und Rechtsprechung liegt allerdings schon länger zurück (April 2016). Man muss aber bedenken, dass Monografien auf diesem Gebiet mehr als rar sind und die Arbeit einen reichen Fundus an Literatur und Rechtsprechung bereithält, so dass man schon allein von dem sehr ausführlichen Fußnotenapparat profitieren kann. Zudem werden de lege ferenda-Vorschläge formuliert, die durchaus auch die aktuelle Diskussion bereichern können.

Der Verfasser macht es sich zur Aufgabe, die Zulässigkeit der Strafverfolgung in sozialen Netzwerken herauszuarbeiten. Dabei legt er einen besonderen Schwerpunkt auf die spezifischen Herausforderungen bei Ermittlungen in sozialen Netzwerken im Unterschied zu sonstigen Ermittlungen in den Kommunikationsdiensten des Internets.

Damit ein einheitliches Begriffsverständnis herrscht, nimmt *Bauer* zunächst eine Begriffserklärung der sozialen Netzwerke sowie eine Beschreibung der Grundfunktionen vor (S. 26 ff.). Auch die technischen Grundlagen werden vermittelt (S. 39 ff.). Dies ist erforderlich, um den Raum und die Grenzen von polizeilichen Ermittlungen technisch abzustecken. Anschließend werden die Möglichkeiten der Nutzung von sozialen Netzwerken als Informationsquelle für Strafverfolgungsbehörden kurz aufgezeigt (S. 47 ff.).

Die nächsten rund 30 Seiten widmet der Autor den verfassungsrechtlichen Anforderungen an strafprozessuale Ermächtigungsgrundlagen. Hier geht es um sehr grundsätzliche Aspekte, wie beispielsweise das Gebot der Normenklarheit und Bestimmtheit, das Analogieverbot oder den Verhältnismäßigkeitsgrundsatz.

Ein erstes Hauptkapitel (S. 98 ff.) beschäftigt sich mit dem Zugriff auf öffentlich zugängliche Daten. Dabei erläutert der Verfasser zunächst den „schillernden" Begriff der Online-Streife, um diesen dann in Bezug zu den öffentlich zugänglichen Daten zu setzen. Er beschreibt die Online-Streife als „passiv beobachtend" (S. 99) und sieht in ihr einen Eingriff in das Recht auf informationelle Selbstbestimmung (S. 121). Mit der herrschenden Meinung geht *Bauer* davon aus, dass die Ermittlungsmaßnahme der Online-Streife auf die Generalermittlungsklausel gem. §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO gestützt werden kann. Zwar könne das Ausforschungspotential aufgrund der mannigfaltigen netzwerköffentlichen Daten hoch sein. Eine Vertraulichkeitserwartung, dass die Daten gar nicht oder nur begrenzt erhoben und verarbeitet werden, bestünde jedoch nicht. Eine Einschränkung macht *Bauer* dann doch: nur soweit keine technischen Mittel zum Auffinden und Erheben der netzwerköffentlichen Daten eingesetzt würden, sei die Online-Streife nach der Generalermittlungsklausel zulässig (S. 146).

In einem weiteren Hauptkapitel widmet sich der Verfasser den verdeckten Ermittlungen (S. 147 ff.), wobei er zwei Vorgehensweisen unterscheidet. Zum einen können die Ermittler ein Profil mit unwahren Angaben – ein sog. Fake-Profil – errichten. Zum anderen können die Ermittler auch ein echtes, bereits existierendes Profil nutzen, das der tatsächliche Nutzer den Strafverfolgungsbehörden freiwillig überlassen hat (sog. verdeckte Identitätsübernahme). Auch hier sieht *Bauer* in beiden Varianten durch die Kommunikationsbeziehung ohne Offenlegung der hoheitlichen Aufgabe einen Eingriff in das Recht auf informationelle Selbstbestimmung (S. 167). Im Folgenden legt er dezidiert dar, dass die §§ 110a ff. StPO im Gegensatz zur überwiegenden Literaturmeinung nicht auf verdeckte virtuelle Ermittler anwendbar sind. Die Argumente sind sehr gut nachvollziehbar und überzeugend. Denn der Aufbau einer virtuellen Legende entspricht nach Auffassung *Bauers* nicht den Anforderungen an den Aufbau einer analogen Legende. Bei einer Identitätsübernahme fehle der Aufbau einer veränderten Identität. Zudem seien die Befugnisse des verdeckten Ermittlers auf körperliche Treffen und nicht auf virtuelle Kommunikation ausgerichtet (S. 198). Auch die Ermittlungsgeneralklausel könne virtuelle verdeckte Ermittlungen in sozialen Netzwerken nicht rechtfertigen (S. 209).

Als Konsequenz dieses Ergebnisses formuliert der Verfasser einen de lege ferenda Vorschlag. Nachdem er die Maßstäbe hierzu abgesteckt hat (S. 209 ff.), folgt ein stimmiger Gesetzesvorschlag eines neu einzufügenden § 110d StPO-E. Dieser lautet wie folgt:

> *„§ 110d StPO-E*
> *(1) Virtuelle verdeckte Ermittler dürfen zur Aufklärung von Straftaten eingesetzt werden, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass die Straftat von erheblicher Bedeutung*
>
> *1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,*
> *2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),*
> *3. gewerbs- oder gewohnheitsmäßig oder*
> *4. von einem Bandenmitglied oder in anderer Weise organisiert*
>
> *begangen worden ist.*
>
> *Zur Aufklärung einer Straftat von erheblicher Bedeutung, die mittels Kommunikation begangen worden ist,*

dürfen virtuelle Ermittler außerdem eingesetzt werden, wenn die besondere Begehung der Tat den Einsatz gebietet. Der Einsatz ist nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Zur Aufklärung von Verbrechen dürfen virtuelle verdeckte Ermittler nach Maßgabe des Absatzes 1 Satz 3 eingesetzt werden.

(2) Virtuelle verdeckte Ermittler sind Beamte des Polizeidienstes, die unter einer virtuell veränderten Identität (virtuelle Legende) in den Kommunikationsdiensten des Internets ermitteln. § 110a Abs. 2 Satz 2 und Abs. 3 gilt entsprechend.

(3) Virtuelle verdeckte Ermittler dürfen sich unter ihrer virtuellen Legende Zugang zu nicht allgemein zugänglichen Bereichen mit dem Einverständnis des Berechtigten verschaffen. Die Zugangsberechtigung eines Dritten darf hierfür nicht genutzt werden (Identitätsübernahme). § 110c Satz 2 und 3 gilt entsprechend. …" (S. 213).

In einem letzten Hauptteil (S. 214 ff.) beschäftigt sich der Verfasser sehr ausführlich mit dem Zugriff auf nichtöffentlich zugängliche Daten. In einem ersten Schritt qualifiziert er sämtliche freiwillige Angaben in sozialen Netzwerken als Inhaltsdaten. Damit unterfallen sie dem Schutz des Art. 10 GG, soweit sie für einen begrenzten Empfängerbereich bestimmt sind (S. 244 f.). Er verneint mit zahlreichen Literaturstimmen die §§ 94 ff. StPO als Eingriffsgrundlage. Erforderlich sei eine auf Art. 10 GG abgestimmte, bereichsspezifische Vorschrift. Er wirft dem *BVerfG* – auch hier ist er nicht alleine – vor, ein „Fernmeldegeheimnis light" geschaffen zu haben. Die fehlende Beherrschbarkeit der Kommunikationsinhalte werde auf strafprozessualer Ebene inkonsequent relativiert (S. 273).

Auch eine direkte oder analoge Anwendung der §§ 99 ff. StPO lehnt *Bauer* ab (S. 281). In einem nächsten Schritt werden die §§ 100a ff. StPO geprüft und für die Überwachung von Nachrichten und Chatinhalten für anwendbar gehalten, da soziale Netzwerke hier als Telekommunikationsdienstleister fungieren. Für die Überwachung anderer Kommunikationsinhaltsdaten seien sie aber als Telemediendienste anzusehen und mangels Nennung in § 100b Abs. 3 StPO nicht zur Mitwirkung verpflichtet. Soweit der Zugriff unter Infiltration des Accounts stattfinde, genügen die §§ 100a ff. StPO nach Auffassung des Autors nicht den verfassungsrechtlichen Anforderungen (S. 316), so dass ein weiterer de lege ferenda Vorschlag formuliert wird. Hierbei wird danach differenziert, ob die Ermittler auf den Account des Nutzers mittels Infiltration oder ohne Infiltration zugreifen. Für letztere Eingriffe reiche eine Änderung des § 100b Abs. 3 StPO und der Kernbereichsprognose aus. Dieser müsse um einen 4. Satz ergänzt werden: „Satz 1 gilt entsprechend für jeden, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt" (S. 317). Bei Eingriffen mit Infiltration sei eine gesetzliche Neuregelung erforderlich (S. 316). Hier formuliert der Verfasser einen ausgewogenen, allerdings sehr ausführlichen de lege ferenda Vorschlag eines § 100k StPO-E auf mehreren Seiten (S. 321 ff.). Ob eine solch explizite Regelung praxistauglich ist, sei einmal dahingestellt. Jedenfalls trägt sie sehr umsichtig der hohen Eingriffsintensität unter Wahrung des Verhältnismäßigkeitsgrundsatzes ausreichend Rechnung.

Nachdem die gesetzlichen Möglichkeiten zu den Inhaltsdaten de lege lata und de lege ferenda aufgezeigt wurden, wird im Folgenden dem Zugriff auf Bestandsdaten nachgegangen (S. 335 ff.). Auch wenn *Bauer* diesbezüglich einen offenen Zugriff über die §§ 94 ff. StPO angesichts der geringen Eingriffsintensität für denkbar hält, spricht er sich doch für eine normklare Neuregelung aus (S. 342). Hier ist die Frage, ob man tatsächlich alles neu formulieren muss, wenn schon Eingriffsgrundlagen in der StPO vorhanden sind und greifen. Als de lege ferenda Vorschlag ist hier vom Autor die Einfügung eines § 100m StPO-E vorgesehen (S. 343). Die immer differenziertere und umfangreichere Anreihung möglicher Ermittlungsmaßnahmen nach §§ 100a ff. StPO lässt unabhängig von der vorliegenden Dissertation die Frage entstehen, ob nicht eine Neuformulierung, Präzisierung und Modernisierung der Ermittlungsmaßnahmen unter besonderer Berücksichtigung des digitalen Fortschritts geboten ist. Hier sind Wissenschaft und Gesetzgebung gefordert, nicht das Stückwerk der strafprozessualen Ermittlungsmaßnahmen fortzusetzen, sondern einheitliche, übersichtliche und praxistaugliche Eingriffsbefugnisse zu schaffen, die trotz dieser Straffung der jeweiligen Eingriffsintensität und dem Verhältnismäßigkeitsgrundsatz Rechnung tragen.

Abschließend widmet sich der Verfasser den Verkehrs- und Nutzungsdaten. Während er für erstere keinen gesetzgeberischen Handlungsbedarf sieht (S. 349), sieht er bei den Nutzungsdaten die Notwendigkeit eines Gesetzentwurfs für einen strafprozessualen Auskunftsanspruch S. 365). Auch hier wird ein de lege ferenda Vorschlag (§ 100n StPO-E) gemacht (S. 369).

Insgesamt, so lässt sich resümieren, ist Handlungsbedarf angezeigt. Die Dissertation legt den Finger in die Wunde unzureichender Ermächtigungsgrundlagen, die den Herausforderungen des digitalen Zeitalters nicht gewachsen sind. *Bauer* macht einen ersten Aufschlag mit zahlreichen de lege ferenda Vorschlägen. Insofern hat sich seine Dissertation auch bei einem Bearbeitungsstand von April 2016 keinesfalls überholt, ganz im Gegenteil bieten die Vorschläge und Ausführungen viel Material für eine kriminalpolitische Diskussion. Allerdings sollte man nicht (nur) über die Gesetzesvorschläge in der Dissertation nachdenken, sondern über eine komplette Revision und Neuformulierung strafprozessualer Ermittlungsmaßnahmen. Denn wie soll es weitergehen, wenn der Gesetzgeber bei § 100z StPO angekommen ist? Übersichtlicher wird es ganz sicher nicht.

Die Dissertation von *Bauer* kann jedem empfohlen werden, der sich kritisch mit strafprozessualen Ermittlungsmaßnahmen in der virtuellen Welt auseinandersetzt. Es ist der Arbeit zu wünschen, dass sie viel rezipiert wird, damit sich schließlich auch der Gesetzgeber der digitalen Neuausrichtung der StPO stellt.