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

Sebastian Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, Duncker & Humblot, Berlin 2018, 406 S., € 89,90.

„Soziale Netzwerke und strafprozessuale Ermittlungen" ist der Titel der Dissertation *Sebastian Bauers*, die 2018 als Band 281 der Reihe „Strafrechtliche Abhandlungen – Neue Folge" erschienen ist.

Sie wurde bereits von *Plank*[1] und *Bär*[2] rezensiert.

Mit ca. 350 Seiten Haupttext handelt es sich um eine durchaus umfangreiche Dissertation. Sie wartet zudem neben Inhalts-, Literatur- und Internetadressenverzeichnis mit einem Stichwortverzeichnis auf.

Gesetzgebung, Rechtsprechung und Literatur befinden sich auf dem Stand von April 2016, was für ein offiziell 2018 (faktisch wohl: Ende 2017) erschienenes Werk schade ist. So finden sich keine Hinweise auf die seit 25.5.2016 in Kraft befindliche und seit 25.5.2018 wirksame Europäische Datenschutz-Reform oder das 2017 in Kraft getretene und allgemein kritisierte Netzwerkdurchsetzungsgesetz. Auch § 100b StPO i.d.F. vom Gesetz vom 17.8.2017 (BGBl. I 2017, S. 3202) ist noch nicht berücksichtigt.

„Soziale Netzwerke und strafprozessuale Ermittlungen" haben vielfältigste Berührungspunkte.

So kann gegen die Betreiber der Netzwerke selbst ermittelt werden. Anlass dafür könnten neben allen „herkömmlichen" Taten, die auch jeder Andere verüben kann, netzwerkspezifische Taten sein – vom Datenmissbrauch über die Beteiligung an Äußerungsdelikten im Netzwerk bis zum Vorwurf der Manipulation demokratischer Wahlen.[3]

Umgekehrt können die Mitglieder der „sozialen Gemeinschaft" als Helfer in Ermittlungen einbezogen werden, indem etwa für bestimmte Mitwirkungshandlungen geworben wird (z.B. Öffentlichkeitsfahndung).[4]

Sicherlich können auch Opfer über „soziale Netzwerke" identifiziert oder Zeugen gefunden werden.

Ermittlungen auslösen können ebenfalls Verhaltensweisen der Nutzer von sozialen Netzwerken. Hinsichtlich deren Online-Aktivitäten sind hier wiederum u.a. Äußerungsdelikte zu nennen.

Aber auch ungeachtet des Inhalts von Äußerungen können Informationen aus sozialen Netzwerken für Ermittler hoch interessant sein, etwa Kontakte, Standorte, zeitliche Zusammenhänge oder verwendete Geräte.

Bauer tut gut daran, sich nicht auf all diese Aspekte einzulassen. Er konzentriert sich auf die letztgenannte Konstellation, also auf Ermittlungen gegen Nutzer sozialer Netzwerke.

Auch die Konzentration auf die strafprozessuale Seite ist nachvollziehbar und dient einem spezifischen Erkenntnisinteresse. In der Praxis freilich dürfte oft eine Gemengelage von strafprozessualen, polizei- und verfassungsschutzrechtlichen Maßnahmen eine Rolle spielen, die dann ineinandergreifen und die Frage aufwerfen, inwieweit in welchem Stadium welche Maßnahmen zur Verfügung stehen und welche Ergebnisse wofür verwertbar sind.

Das Werk Bauers gliedert sich in sechs Kapitel (A–F).

Zunächst (A) wird neben funktionalen und technischen Grundlagen erörtert, in welchen Konstellationen Ermittlungen denkbar sind – etwa offene und heimliche Maßnahmen.

Kapitel B widmet sich den verfassungsrechtlichen Fragen. Spätestens seit dem 25.5.2018, als die Richtlinie (EU) 2016/680 (JI-RL) wirksam wurde, wird auch Unionsrecht zu berücksichtigen sein. Dies wird aber, weil „der Datenschutz" in Deutschland schon auf hohem Niveau ist, voraussichtlich nicht zu gravierenden Änderungen führen.

In Kapitel B geht *Bauer* u.a. der Frage nach, ob es im Strafprozessrecht ein Analogieverbot gibt (S. 78 ff.). Er stellt die uneinheitliche Rechtsprechung und die Literaturmeinung (die ein Analogieverbot eher befürwortet) vor und begründet schließlich, weshalb auch er ein solches Analogieverbot vertritt (S. 81). Dessen eigentliche Stütze sei im Grundsatz des Vorbehalts des Gesetzes zu sehen.

In Kapitel C wird der Zugriff auf öffentlich zugängliche Daten behandelt.

Teilweise missverständlich erscheinen einige Aussagen zu Art. 10 GG:

- Art. 10 GG schütze „das Abhörrisiko" (S. 100, 101). Natürlich schützt er nicht das Risiko, sondern die Freiheit vor Abhörmaßnahmen.
- Art. 10 GG schütze nicht die Vertraulichkeit der Kommunikation mit dem Staat (S. 149). Das mag mit Blick auf die „Online-Streife" richtig sein. Der Aussage ist aber entgegenzuhalten, dass „der Staat" sich in viele verschiedene Körperschaften, Behörden usw. aufteilt. Kommuniziert der Bürger (bewusst) mit einer davon, so schützt Art. 10 GG durchaus vor dem Abhören durch eine andere staatliche Stelle.

Kapitel C schließt mit der Feststellung, das Sammeln offen zugänglicher Daten greife in das Recht auf informationelle Selbstbestimmung ein, wobei die Intensität des Eingriffs weniger von der Heimlichkeit als vom sammelnden Mittel abhänge: der Einsatz eines technischen Mittels wiege schwerer. Hier dürfte die Vorstellung eines „manuell suchenden" Polizeibeamten im Gegensatz zu einem softwaregestützten „Social Media Monitoring"[5] leitend sein. Dass letztere intensiver eingreift, ist tendenziell sicher richtig. Allerdings bedient sich die „manuelle Suche" ebenfalls technischer Mittel, nämlich der plattforminternen Suchfunktion.

[1] Rezension abrufbar unter http://polizei-newsletter.de/wordpress/?p=902 (18.6.2018).
[2] *Bär*, MMR-Aktuell 2018, 405095.
[3] Siehe die Skandale um Facebook, https://www.n-tv.de/politik/EU-will-gegen-Wahlmanipulation-kaempfen-article20463764.html (18.6.2018).
[4] Dazu *Bajmel*, Datenschutz in sozialen Netzwerken: Die Öffentlichkeitsfahndung im Rahmen der Nutzung des sozialen Netzwerkes Facebook, 2017.
[5] Dazu *Ziebarth*, SchuR 2016, 9.

Weiter werden verdeckte Ermittlungen (D) und Zugriff auf nichtöffentlich zugängliche Daten (E) unterschieden. Dabei ist zu beachten, dass sowohl öffentlich als auch nicht öffentlich zugängliche Daten jeweils mit oder ohne Kenntnis des Betroffenen erhoben, gespeichert, ausgewertet oder weitergegeben werden können.

Die Verarbeitung kann zudem auch mit oder ohne Kenntnis des Portalbetreibers geschehen, wobei dessen mangelnde Kenntnis sich weniger auf den Verarbeitungsvorgang beziehen wird, als auf die amtliche Eigenschaft des Ermittlers.

Kapitel D endet mit einem Vorschlag eines § 110d StPO-E. Gesetzesvorschläge scheinen in Dissertationen beliebt zu sein. Das erscheint mäßig nützlich und macht angreifbar, weil Unstimmigkeiten in so komplexen Entwürfen kaum vermeidbar sind. Im Entwurf von § 110d Abs. 1 ist z.B. jedenfalls dem Rezensenten unklar, in welchem Verhältnis die Voraussetzungen für den Einsatz „virtueller verdeckter Ermittler" im Hinblick auf die Katalogtaten nach Satz 1 gegenüber den Voraussetzungen im Hinblick auf alle (?) Verbrechen nach Satz 4 stehen sollen.

Auch Kapitel E endet mit einem Gesetzesvorschlag hinsichtlich eines neuen § 100k StPO-E. Auch dieser Entwurf erklärt „die Maßnahme" für unzulässig, wenn sie kernbereichsrelevante Inhalte zutage zu fördern droht. Dies entspricht der Rechtslage u.a. gem. § 100d Abs. 1 StPO. Dennoch geht dieser Schutz zu weit: Es wäre ausreichend, eine einzelne Datenerhebung innerhalb der Maßnahme abzubrechen, wenn sich bei dieser Erhebung Anhaltspunkte für eine Kernbereichsrelevanz fänden.[6] Dass Maschinen (Rechner, Software) kernbereichsrelevante Daten hinreichend sicher identifizieren könnten, erscheint unrealistisch.[7]

Abgeschlossen wird die Dissertation durch die Darstellung von Gesamtergebnis und Schlussbemerkung (F).

Die hier punktuell geübte Kritik soll nicht darüber hinwegtäuschen, dass die Dissertation *Bauers* ihr aktuelles und wichtiges Thema grundlegend aufbereitet. *Bauer* geht auch dogmatisch in die Tiefe und stellt sich schwierigen verfassungsrechtlichen Fragen. Meinungsunterschiede im Detail sind nicht zu vermeiden.

Keine Meinungsverschiedenheiten sollte es in der Bewertung geben, dass die Dissertation *Bauers* ein gut gelungenes Werk ist, dessen Lektüre fachlich Interessierten in jedem Falle zu empfehlen ist.

Dr. Wolfgang Ziebarth, Mannheim

[6] *Ziebarth*, Online-Durchsuchung, 2013, S. 103, 193 ff., 202.
[7] *Ziebarth* (Fn. 6), S. 104 ff.