

## Verdeckte Ermittlungen

mit Ausblick auf landesrechtliche Vorschriften

Bearbeitet von  
Von Prof. Dr. Ursula-Isabel Grün, LL.M.

1. Auflage 2018. Buch. XXVII, 216 S. Kartoniert  
ISBN 978 3 406 71967 7  
Format (B x L): 16,0 x 24,0 cm  
Gewicht: 447 g

[Recht > Strafrecht > Strafrecht allgemein, Gesamtdarstellungen](#)

Zu [Inhalts-](#) und [Sachverzeichnis](#)

schnell und portofrei erhältlich bei

  
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung [beck-shop.de](http://beck-shop.de) ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

### III. Befugnisse

#### 1. Auftreten im Rechtsverkehr

Gemäß § 110a II 2 StPO dürfen VE unter ihrer Legende am Rechtsverkehr teilnehmen. Dazu gehört auch die Eingehung vertraglicher Verpflichtungen wie zB der Abschluss von Kauf- oder Mieterträgen.<sup>36</sup> Weitere Beispiele sind die Beantragung gewerblicher Erlaubnisse sowie Einträge in öffentliche Register wie das Handelsregister. Ferner kann der VE unter seiner Legende klagen und verklagt werden. 34

§ 110a III StPO sieht vor, dass zum Aufbau sowie zur Aufrechterhaltung der Legende die dafür erforderlichen Urkunden hergestellt, verändert und gebraucht werden dürfen. Der VE macht sich daher nicht strafbar, wenn er einen falschen Personalausweis, Reisepass und Führerschein nutzt. Zudem kann die Erstellung nebst Nutzung weiterer Urkunden erforderlich sein zB betreffend den (angeblichen) schulischen oder beruflichen Werdegang.<sup>37</sup> Wird der VE aufgrund solcher Dokumente eingestellt, kann er deshalb hernach strafrechtlich weder wegen etwaiger Urkundsdelikte nach §§ 267 ff. StGB belangt werden noch wegen eines Eingehungsbetruges nach § 263 StGB gegenüber dem gutgläubigen Arbeitgeber. Keine Strafbarkeit haben insoweit auch die „Helfer“ des VE zu befürchten: Personen, welche die erforderlichen „Tarnpapiere“ für den Aufbau und die Aufrechterhaltung der Legende herstellen, können aufgrund der Ermächtigung des § 110a III StPO nicht wegen § 348 StGB belangt werden.<sup>38</sup> 35

#### 2. Betreten von Wohnungen

Soll der VE eine Wohnung betreten, sind § 110c S. 1 und 2 StPO zu beachten. Danach darf der VE eine Wohnung unter Verwendung seiner Legende betreten. Das gilt allerdings nur, wenn der Wohnungsinhaber damit einverstanden ist. Mehr als die bloße Täuschung über seine Identität ist dem VE in diesem Zusammenhang nicht gestattet. Das schließt ein heimliches oder aber gewaltsames Betreten von Wohnungen durch einen VE aus.<sup>39</sup> Und auch das Vortäuschen eines Zutrittsrechts kommt nicht in Betracht. 36

► **Fall:** Ein VE wurde auf den mutmaßlichen Mafiosi und Bandenchef M angesetzt. Die Polizei hat Grund zu der Annahme, dass sich das Logistikzentrum des Clans im Keller des Hauses von M befindet. Der VE überlegt, ob er sich an der Türe des Beschuldigten als Gasableser oder sonst als städtischer Bediensteter ausgeben darf, um sich so zeitnah Zutritt zum Gebäude des M zu verschaffen und weitere Anhaltspunkte für die Strafverfolgung zu erhalten; ginge das?

**Lösung:** Nein; § 110c S. 2 StPO untersagt dies explizit. Erfordert der Einsatz des VE ein Betreten der Wohnung, wird der Polizeibeamte folglich warten müssen, bis ihn der M gegebenenfalls von sich aus einlädt. Nicht aber darf

<sup>36</sup> S. hierzu und zum Folgenden MüKoStPO/Günther § 110a Rn. 34 f.

<sup>37</sup> MüKoStPO/Günther § 110a Rn. 38.

<sup>38</sup> Meyer-Goßner/Schmitt/Schmitt StPO § 110a Rn. 8.

<sup>39</sup> Meyer-Goßner/Schmitt/Schmitt StPO § 110b Rn. 4.

ein Betreten dadurch erwirkt werden, indem sich der VE kurzerhand als Beamter oder Angehöriger einer staatlichen Einrichtung ausgibt.<sup>40</sup>

### 3. Sonstige Befugnisse und Verpflichtungen

- 37 § 110c S.3 StPO stellt klar, dass für den VE auch während seines Einsatzes die allgemeinen polizeilichen Verpflichtungen und Befugnisse fortgelten.
- 38 Die **Befugnisse** richten sich nach der Strafprozessordnung sowie anderen Rechtsvorschriften. Zu letzteren zählen die jeweiligen Polizeigesetze und sonstige Gesetze bzw. Vorschriften wie beispielsweise § 4 II BtMG.<sup>41</sup>

**Beispiele:** Folge davon ist unter anderem, dass strafprozessuale Zwangsmaßnahmen wie zB eine Durchsuchung oder eine Beschlagnahme lediglich unter den Voraussetzungen der §§ 102 ff. bzw. §§ 94 ff. StPO durchgeführt werden dürfen. Dies bedeutet, dass sich ein VE „offen“ als Polizeibeamter zu erkennen geben muss, will er im Einzelfall von Zwangsbefugnissen Gebrauch machen.<sup>42</sup> Gleiches gilt, wenn er eine vorläufige Festnahme nach § 127 II StPO plant. Weil der VE dadurch seine Legende gefährdet, wird er zu derartigen Mitteln nur im äußersten Notfall greifen.<sup>43</sup> Um den Einsatz des VE nicht zu gefährden bietet sich eine andere Möglichkeit an; nämlich dass Kollegen offen einschreiten. Die Legende des VE bleibt auf diese Weise unangetastet.

Bei der Verfolgung von Organisierter Kriminalität erstreckt sich die Tätigkeit des VE ferner auf Initiativermittlungen (vgl. RiStBV Anlage E Nr. 6).<sup>44</sup>

Zudem ist es dem VE auch im Rahmen seiner strafverfolgenden Tätigkeit gestattet, präventivpolizeilich tätig zu werden.<sup>45</sup>

- 39 Den VE trifft eine **Strafverfolgungspflicht**. Allein die Tätigkeit als VE entbindet diesen nicht von der Pflicht eines jeden Polizeibeamten nach § 163 StPO, bekanntgewordene Straftaten zu erforschen (vgl. Anlage D zur RiStBV Nr. II. 2.6). Um den VE zu schützen ist es aber möglich, Ermittlungsmaßnahmen zeitweilig zurückzustellen. Das Legalitätsprinzip enthält zwar eine Pflicht zum Einschreiten. Jedoch gebietet es zumeist kein sofortiges Einschreiten und gilt auch sonst nicht lückenlos. Beleg dafür sind explizit die in §§ 153 ff. StPO gesetzlich verankerten Möglichkeiten der Staatsanwaltschaft, ein Verfahren einstweilen oder dauerhaft einzustellen. Anlage D zur RiStBV Nr. II. 2.6. sieht daher vor, dass Ermittlungsmaßnahmen aus kriminaltaktischen Erwägungen zurückgestellt werden können. Das gilt sowohl für Maßnahmen, die in den Auftrag des VE fallen (RiStBV Nr. II. 2.6.1) als auch für Zufallsfunde, welche der VE bei Gelegenheit seiner Tätigkeit macht (RiStBV Nr. II. 2.6.2). Allerdings darf nicht so lange zugewartet werden, bis die Tat nicht mehr verfolgbar ist. Zudem

<sup>40</sup> Meyer-Goßner/Schmitt/Schmitt StPO § 110c Rn. 1.

<sup>41</sup> Zu § 4 II BtMG vgl. die Ausführungen unter → 10. Kap. Rn. 46 f.

<sup>42</sup> Hilger NStZ 1997, 449 (450).

<sup>43</sup> S. hierzu und zum Folgenden *Rachor* in Lisken/Denninger PolR-HdB Kap. E Rn. 256.

<sup>44</sup> BeckOK StPO/Hegmann, 28. Ed. 24.8.2017, § 110c Rn. 5.

<sup>45</sup> BT-Drs. 12/2720, 47.

kann es Sachverhalte geben, in denen ein sofortiges Einschreiten wegen der Schwere der entdeckten Tat geboten ist (RiStBV Nr. II. 2.6.2).

► **Fall:** VE Sorgsam (= S) hat den Auftrag, die Strukturen einer Bande aufzudecken, die illegal in großem Stil mit Schusswaffen handelt. Er kann gerade erste Erfolge verbuchen. Da erfährt er anlässlich eines Kneipenabends mit der Clique, dass ein Bandenmitglied „nebenberuflich“ wertvolle Motorräder und Luxus-sportwagen stiehlt. Er erfährt weiter, wo das Diebesgut zwischengelagert wird. S ist klar, dass seine umgehende Enttarnung droht, sollte die Polizei in Sachen entwendeter Sportwagen und Co. ausgerechnet jetzt zeitnah nach besagter Info an ihn einen Ermittlungserfolg verbuchen. Schließlich gibt es außer dem S derzeit keine Neuzugänge beim Waffenschieberring. Wie verhält S sich richtig?

**Lösung:** Sobald der VE dies gefahrlos tun kann, muss er sich an seinen VE-Führer wenden und diesem seine Erkenntnisse mitteilen. Gewisse Verzögerungen bei der Weitergabe der Informationen sind dem VE aus Eigenschutzgründen zuzugestehen und notfalls auch über § 34 StGB gedeckt. Die Weitergabe der Informationen hat zur Folge, dass dem VE keine Bestrafung wegen Strafvereitelung im Amt durch Unterlassen (§§ 258a, 13 StGB) droht. Der VE-Führer klärt dann seinerseits umgehend mit der Staatsanwaltschaft die weitere Verfahrensweise ab. Nur diese ist befugt, ein Verfahren wegen des Zufallsfundes beispielsweise nach § 154 StPO vorläufig einzustellen. Ist dagegen in einem Fall je ein sofortiges Einschreiten geboten, bleibt nur der sofortige Abbruch des VE-Einsatzes, ehe die Strafverfolgungsbehörden einschreiten.

#### 4. Grenze Straftatbegehung

Der VE darf selbst generell keine Straftaten begehen. Dies klingt nach einer Selbstverständlichkeit, immerhin ist er Polizeibeamter. Allerdings zeitigt dieses Verbot für den VE in der Einsatzpraxis Konsequenzen: Das gilt zB dann, wenn es um eine „Keuschheitsprobe“ geht, damit er Aufnahme in den anvisierten kriminellen Kreis erlangt. Das wird er – möglichst geschickt – ablehnen müssen. 40

Nicht verboten ist jedoch das Vortäuschen der Begehung von Straftaten.<sup>46</sup> Das eröffnet verdeckt arbeitenden Polizeibeamten gewisse Spielräume. 41

**Beispiel** dafür sind etwa verdeckt geführte Ermittlungen im Internet. So können die Ermittler versuchen, Zugang zu geschlossenen Chat-Gruppen zu erhalten, indem sie zwecks Aufnahme in den Kreis „Bild“-Dateien verschicken, welche sich nicht öffnen lassen oder Ähnliches.<sup>47</sup> Der Ermittler kann dann behaupten, die Bild-Proben hätten angeblich den gewünschten illegalen Inhalt.

Untersagt sind ferner „milieubedingte“ Straftaten.<sup>48</sup> Der VE wird sich infolgedessen etwas einfallen lassen müssen, um sich der Begehung oder Teilnahme 42

<sup>46</sup> OLG Zweibrücken NStZ 2011, 113 (114).

<sup>47</sup> Zum VE als Instrument zur Bekämpfung von Kinderpornographie im Internet *Soiné* NStZ 2003, 225 (226 ff.).

<sup>48</sup> Meyer-Goßner/Schmitt/Schmitt StPO § 110c Rn. 4.

an Delikten zu entziehen, welche in den einschlägigen Kreisen typischerweise (wiederholt) begangen werden. Beispiel dafür ist das unerlaubte Glücksspiel, welches sich im Milieu großer Beliebtheit erfreut.<sup>49</sup> Der mitunter bemühte Ansatz, die Teilnahme des VE am illegalen Glücksspiel sei schon nicht tatbestandsmäßig iSv §285 StGB,<sup>50</sup> überzeugt insoweit nicht. Ein und dasselbe Spiel kann nicht – je nach beteiligter Person – mal unerlaubt und dann wieder erlaubt sein.<sup>51</sup>

- 43 Lediglich wenn im Einzelfall eine nicht anders abwendbare Gefahr speziell für Leib, Leben und Freiheit des VE droht, ist es möglich, dessen Handeln **ausnahmsweise** nach §§32 oder 34 StGB als gerechtfertigt oder aber nach §35 StGB als entschuldigt anzusehen.<sup>52</sup> Nicht ausreichend ist dagegen der bloße Wunsch nach dem Aufrechterhalten der Legende.<sup>53</sup> Wegen des hohen Rangs des Legalitätsprinzips sind Beschränkungen der Handlungsmöglichkeiten des VE unumgänglich.<sup>54</sup>

## E. Sonderkonstellationen/-probleme

### I. Ermittlungen im Internet

- 44 Recherchen im Internet gehören längst zum polizeilichen Alltag (dazu bereits → 3. Kap Rn. 50 ff.). Gleiches gilt für weitere Ermittlungsmaßnahmen wie zB Scheinkäufe im Netz.<sup>55</sup> Sofern Polizeibeamte jenseits der allgemein zugänglichen Datenbestände unter Verwendung falscher Namen recherchieren bzw. agieren, stellt sich die Frage, wie diese Funktion zu kategorisieren ist. **Zumeist** werden die „Cybercops“<sup>56</sup> dann als virtueller NoeP eingestuft. Das bedeutet, dass Ermittler, die im Internet nur gelegentlich unter einem Decknamen auftreten und in offenen Chatrooms oder sozialen Netzwerken mit anderen Teilnehmern kommunizieren, generell keiner Anordnung nach §§110a ff. StPO bedürfen.<sup>57</sup> Insoweit bildet §163 StPO die Grundlage des polizeilichen Handelns mittels eines legendierenden Accounts.
- 45 Eine andere Sicht der Dinge ist jedoch geboten, wenn Polizeibeamte im Netz über einen längeren Zeitraum unter einer umfassenden Legende auftreten **und** ihnen aufgrund besagter Legende die Überwindung stichhaltiger Zugangskontrollen etwa zu einem geschlossenen Internetforum gelingt. Aufgrund der

<sup>49</sup> Hund NStZ 1993, 571.

<sup>50</sup> Hund NStZ 1993, 571 (572); Meyer-Goßner/Schmitt/Schmitt StPO §110c Rn. 4.

<sup>51</sup> Zutr. BeckOK StGB/Feilcke/Hollering, 36. Ed. 1.11.2017, §285 Rn. 6 mwN zum Meinungsstand.

<sup>52</sup> Meyer-Goßner/Schmitt/Schmitt StPO §110c Rn. 4 mwN; Schwarzburg NStZ 1995, 469 (472).

<sup>53</sup> Trurnit Die Polizei 2015, 255 (260).

<sup>54</sup> Vgl. KK-StPO/Bruns §110c Rn. 6 mwN zum gesetzgeberischen Willen.

<sup>55</sup> → 10. Kap. Rn. 46 f.

<sup>56</sup> Ausdruck für Ermittler im Internet, vgl. Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl. 2010, Rn. 515.

<sup>57</sup> Vgl. KK-StPO/Bruns §110a Rn. 7; Meyer-Goßner/Schmitt/Schmitt StPO §110a Rn. 4; das BVerfG NJW 2008, 822 Rn. 311 sieht in einer reinen Internetaufklärung nicht einmal einen Grundrechtseingriff.

vorgeschalteten Überprüfungsmechanismen glauben die anderen Teilnehmer, die Identität und die Motivation des neu Hinzugekommenen zu kennen. In solchen Sachverhalten ist das Vertrauen der Betroffenen, nicht mit einer staatlichen Stelle zu kommunizieren, schutzwürdig (→ 3. Kap. Rn. 52). Daher erfordert die aktive Erhebung von Informationen durch einen längerfristig unter einer Legende arbeitenden Ermittler jedenfalls dann eine Anordnung gem. §§ 110a ff. StPO, wenn die Identität des Partners bei der Aufnahme in eine geschlossene Benutzergruppe eine ernst zu nehmende Rolle gespielt hat (virtueller VE).<sup>58</sup> Nicht ausreichend sind dafür lediglich rein formale Zugangskontrollen. Denn wenn ohne weiteres Nicknames oder Ähnliches akzeptiert werden, bleiben die angemeldeten Personen genau besehen weiterhin „anonym“. Hier besteht kein schutzwürdiges Vertrauen in die Identität des Gegenübers.

## II. Scheinkäufe und -verkäufe

### 1. Grundlagen

Tätigen verdeckt ermittelnde Polizeibeamte Scheinkäufe explizit im BtM-Bereich, droht ihnen deswegen keine Strafbarkeit. § 4 II BtMG gestattet polizeiliche Scheingeschäfte von NoeP sowie von VE. Der Einholung einer vorherigen Erlaubnis bedarf es nicht. Allerdings erfolgen solche inszenierten Käufe in der Praxis zumeist dennoch nicht spontan – werden die handelnden Beamten doch in aller Regel vorab mit Vorzeige- und mit Kaufgeld für solche Geschäfte ausgestattet.<sup>59</sup> Erlaubt ist ferner der Transport solchermaßen erworbener Drogen zum Zwecke der Sicherstellung. Für förmlich verpflichtete V-Leute gilt die Regelung entsprechend.<sup>60</sup>

Nicht gestattet ist dagegen die Weitergabe von Drogen, etwa zur Legendenbildung durch einen VE.<sup>61</sup> Im Wege von Scheingeschäften gekaufte oder zuvor bereits in anderen Verfahren sichergestellte Drogen können von der Polizei infolgedessen nicht im Zuge eines VE-Einsatzes zB zum Zwecke der „Keuschheitsprobe“ genutzt werden.

### 2. Aktuelle Tendenzen

In der Praxis verlagert sich der Handel mit illegalen Gütern wie explizit Drogen, Waffen, Falschgeld uvm in den letzten Jahren sprunghaft in immer stärkerem Maße ins Internet, genauer: ins Darknet. Wurde zur Abwicklung der Geschäfte zunächst eher die verschlüsselte Internettelefonie (VoIP, HTTPS) bemüht,<sup>62</sup> erfolgt nicht nur der Drogenhandel zwischenzeitlich oft – noch unkomplizierter – über entsprechende illegale Shops im Darknet,<sup>63</sup> der Grund: Das „dunkle

<sup>58</sup> BVerfG NJW 2008, 822 (836) Rn. 310 f.; Meyer-Goßner/Schmitt/Schmitt StPO § 110a Rn. 4; KK-StPO/Bruns § 110a Rn. 7.

<sup>59</sup> Soine NStZ 2010, 596 (601).

<sup>60</sup> Vgl. Körner/Patzak/Volkmer/Patzak BtMG § 4 Rn. 34; Es genügt insoweit auch eine dahingehende präzise (An-)Weisung der VP.

<sup>61</sup> Körner/Patzak/Volkmer/Patzak BtMG § 4 Rn. 37.

<sup>62</sup> Müller Kriminalistik 2012, 295 (297).

<sup>63</sup> Ries c't 2016, 68 ff.

Netz“ ist nicht ohne Weiteres zugänglich. Das stellt einen gravierenden Unterschied zum „normalen“ Internet (Visible Web) dar. Erreichbar ist das „dunkle“, unsichtbare Netz ausschließlich über spezielle Anonymisierungsnetzwerke. Das wohl bekannteste Darknet ist das Tor-Netzwerk. Dieses wird mit dem TOR-Browser („The Onion Router“) erschlossen.<sup>64</sup> Jener ist frei im Internet verfügbar und absolut legal. Wird er installiert, können die Nutzer sich hernach verschlüsselt und völlig anonym im TOR-Netzwerk bewegen. Auch im Zuge von Kauf- und Verkaufsaktivitäten wird die Identität der Akteure nicht bekannt, da sich im Darknet jeder mit einem Nickname und einem Passwort registrieren kann. Echte Identitäten werden demgegenüber nicht preisgegeben. „Sicherheit“ betreffend die Angebote wird etwa dadurch gewährleistet, dass Käufer den Betrag zunächst auf ein Treuhandkonto (escrow) zahlen. Zum Schutz vor Betrug kann sich der Kunde zudem Bewertungen der jeweiligen Shops bzw. Markets ansehen. Bevorzugte Zahlungsmittel sind sog. (echte) virtuelle Zahlungssysteme wie spezielle Bitcoins.<sup>65</sup> Charakteristisch für die Bitcoin-Währung ist die Freiheit von einer zentralen Kontrollinstanz oder Ausgabestelle. Im Unterschied zu regulären Zahlungssystemen hat die virtuelle Währung den Vorteil der Pseudonymität.<sup>66</sup> Das „passt“ zu den Geschäftspraktiken der Händler und Käufer im Darknet.

- 49 Sicherheitsbehörden weltweit ist es bisher nicht gelungen, das TOR-Netzwerk auszuhebeln. Die Verschlüsselung kann technisch bislang nicht „geknackt“ werden.<sup>67</sup> Auch können die TOR-Server nicht einfach so abgeschaltet werden. Soll den Betreibern von Drogen- und Waffenshops das Handwerk gelegt werden, bleibt den Ermittlern daher nur der mitunter mühsame Weg über klassische Ermittlungstechniken. Hierbei spielen insbesondere „verdeckte Personalermittlungen“ eine Rolle. Mit Einzelmaßnahmen wie beispielsweise über Scheinkäufe versuchen Strafermittler, Kriminelle im Darknet zu identifizieren.<sup>68</sup> Erste Erfolge konnten die Ermittler bereits verbuchen. So existiert die „Silk Road“, einer der großen virtuellen Schwarzmärkte im Darknet, zwischenzeitlich nicht mehr.<sup>69</sup> Das bedeutet aber nicht, dass das Problem des Handels mit illegalen Substanzen usw. im Darknet damit behoben wäre. Im Gegenteil vertreiben auf diesem Weg immer neue Anbieter ihre keineswegs legalen Waren.<sup>70</sup> Dazu gesellen sich weitere illegale Aktivitäten: „Zum Standard“ zählen

<sup>64</sup> Vgl. hierzu und zum Folgenden *Rath* DRiZ 2016, 292 (293).

<sup>65</sup> Zu den Grundlagen und der Funktionsweise dieser virtuellen Währung vgl. *Jänke* Kriminalistik 2016, 63 ff.; s. ferner *Boehm/Pesch* MMR 2014, 75 ff.; andere virtuelle Zahlungssysteme sind Second Life oder auch Online Casinos.

<sup>66</sup> *Boehm/Pesch* MMR 2014, 75 (76); zu gleichwohl bestehenden Ermittlungsmöglichkeiten vgl. *Jänke* Kriminalistik 2016, 63 (66) sowie DPZ 2/2017, 7.

<sup>67</sup> S. dazu sowie nachfolgend *Dittert/Mosßbrucker*, Darknet – Mythos und Realität, Reise in den digitalen Untergrund; <https://www.tagesschau.de/inland/darknet-reise-in-die-digitale-unterwelt-101.html>.

<sup>68</sup> *Rath* DRiZ 2016, 292 (293).

<sup>69</sup> Ausf. dazu *Scherschel*, Anonymer Handelsplatz Silk Road durch Programmierfehler aufgefliegen; <https://www.heise.de/security/meldung/Anonymer-Handelsplatz-Silk-Road-durch-Programmierfehler-aufgeflogen-2369631.html>; s. ferner *Jänke* Kriminalistik 2016, 63 (65 f.).

<sup>70</sup> Weitere Beispiele benennt *Ries* in c't 2016, 68 ff.



„Crime as a Service“-Angebote. Diese eröffnen auch technisch nicht versierten Kunden die Möglichkeit, sich mit wenigen Eingaben und Clicks binnen Kürze kriminelle Werkzeuge wie zB Verschlüsselungs- und Erpressungs-Trojaner („Ransomware“) wunschgerecht erstellen zu lassen.<sup>71</sup> Und auch der Tausch von Kinderpornographie über eigens dafür eingerichtete geschlossene Netzwerke stellt bedauerlicher Weise ein kriminelles Betätigungsfeld dar.<sup>72</sup>

Die Ermittler passen sich an und dringen ebenfalls ins Darknet vor. Teils sehen sie sich einfach nur um. Teils versuchen sie, strafrechtlich relevante Sachverhalte weiter zu erforschen; das kann in Form der Teilnahme an der Internetkommunikation geschehen. Oder aber die Ermittler treten unter einem legendierenden Account als Scheinkäufer auf – zumeist als virtueller NoeP (→ 10. Kap. Rn. 44). Neben Drogenkäufen sind ferner Scheinkäufe von Waffen, Falschgeld, Fälscherwerkzeugen, un versteuerten Zigaretten, Arzneien usw möglich.<sup>73</sup> Weil die gefährlichen/illegalen Gegenstände so nicht in Umlauf kommen, machen sich Polizisten als Scheinkäufer insoweit nicht strafbar. Dies gilt selbst in Sachverhalten, in denen für den Ankauf des konkreten Handelsguts im Einzelfall keine spezielle Befugnisnorm vergleichbar der Vorschrift des § 4 II BtMG (→ 10. Kap. Rn. 46) existiert.<sup>74</sup>

50

**Merke:** Mag das Darknet auch durch Verschlüsselung gesichert sein. Selbst die dort tätigen Kriminellen machen Fehler. Mitunter begehen sie diese im Netz, sodass hierdurch ungewollt ihre wahre Identität offenbar wird.<sup>75</sup> Besondere Bedeutung kommt bei Scheinkäufen des Weiteren der Schnittstelle zur realen Welt zu: Beispiel dafür ist etwa die mehrfache Nutzung ein und derselben Packstation zur Übergabe bestellter Waren.<sup>76</sup> Entscheidend für den Ermittlungserfolg können ferner Fingerabdrücke oder DNA-Spuren auf der Ware oder am Paket sein, Hinweise von Informanten, Funde im Rahmen von Durchsuchungen uvm.<sup>77</sup>

Zulässig ist überdies das Auftreten als Schein-Verkäufer. Da Polizeibeamte generell und somit auch im Darknet keine Straftaten begehen dürfen, sind einem solchen Vorgehen indes von vornherein enge Grenzen gesetzt. Schein-Angebote

51

<sup>71</sup> Vgl. Scherschel Ransomware-as-a-Service: Mit Satan den eigenen Erpressungstrojaner bauen; <https://www.heise.de/security/meldung/Ransomware-as-a-Service-Mit-Satan-den-eigenen-Erpressungstrojaner-bauen-3605326.html>.

<sup>72</sup> Rath DRiZ 2016, 292 (293).

<sup>73</sup> Grdl. dazu BGH NSTZ 1995, 516f.; vgl. ferner Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2015, Rn. 1646.

<sup>74</sup> Rath DRiZ 2016, 292 (293) unter Verweis auf die Rechtsprechung des BGH.

<sup>75</sup> Beispiel dafür ist die Silk Road, vgl. Scherschel, Anonymer Handelsplatz Silk Road durch Programmierfehler aufgefliegen; <https://www.heise.de/security/meldung/Anonymer-Handelsplatz-Silk-Road-durch-Programmierfehler-aufgefliegen-2369631.html> (zuletzt abgerufen am 11.7.2017).

<sup>76</sup> Dittert/Moßbrucker, Darknet – Mythos und Realität, Reise in den digitalen Untergrund; <https://www.tagesschau.de/inland/darknet-reise-in-die-digitale-unterwelt-101.html> (zuletzt abgerufen am 11.7.2017).

<sup>77</sup> Rath DRiZ 2016, 292 (293).



als Reaktion auf eine dahingehende individuelle Anfrage – zB in einem Forum – werden noch für zulässig erachtet.<sup>78</sup> Darüber hinaus ist aber Vorsicht geboten. Zu weit ginge die Errichtung eigener (Fake-)Shops im Darknet. Einem solchen Vorgehen würde bildlich gesprochen der Geruch der unerlaubten Tatprovokation anhaften (vertiefend → 10. Kap. Rn. 52 ff.).

### III. Tätigkeit als agent provocateur

#### 1. Allgemeines

- 52 Mit dem Begriff des agent provocateur bzw. „Lockspitzel“ wird eine **spezielle Taktik** umschrieben, welche sowohl von VE aber ebenso von NoeP oder V-Leuten zu Zwecken der Strafverfolgung angewandt werden kann.<sup>79</sup> Die Aufgabe eines Lockspitzels besteht darin, einen **Verdächtigen zu einer strafbaren Handlung zu verleiten**. Aufgrund dieser neuen, „provoozierten“ Tat soll der Verdächtige sodann überführt werden. Dies bedeutet, dass die verdeckt ermittelnde Person die Tatbereitschaft gezielt wecken muss. Ausreichend kann ferner die Intensivierung einer Tatplanung durch den Lockspitzel sein.<sup>80</sup> Nicht aber genügt das schlichte Ausnutzen eines bereits bestehenden, offen erkennbaren Tatentschlusses.<sup>81</sup> Insoweit fehlt es an einer echten Einflussnahme auf die Willensbildung und somit an einer Provokation zur Tat.
- 53 Gemäß der ständigen Rechtsprechung liegt darüber hinaus selbst dann (noch) kein tatprovoozierendes Verhalten vor, wenn eine verdeckt agierende Person einen verdächtigen Dritten (einmalig) und ohne sonstige Einwirkung schlicht darauf anspricht, ob dieser zB Drogen beschaffen könne.<sup>82</sup>

#### 2. Grenzen des Lockspitzeleinsatzes

- 54 Der Einsatz von polizeilichen Lockspitzeln verkörpert eine rechtlich schwierige Thematik. Aufgabe der Polizei ist es an sich, Straftaten zu untersuchen sowie deren Begehung falls möglich zu verhindern. Nicht aber zählt die Anstiftung zu neuen Straftaten zum Aufgabenkreis der Polizei.<sup>83</sup> Dessen ungeachtet billigt die höchstrichterliche Rechtsprechung tatprovoozierendes Verhalten als Ermittlungsmaßnahme zur Aufklärung besonders gefährlicher und schwer aufklärbarer Formen der Kriminalität.<sup>84</sup> Notwendig ist dies deshalb, weil es in manchen Deliktsbereichen kaum erfolgversprechende Alternativen für die Ermittler gibt. So erstatten zB betroffene Opfer im Bereich des Drogenhandels generell keine Strafanzeigen.<sup>85</sup> Hier und in anderen Bereichen wie etwa bei Auftragsdiebstählen wertvoller Kunstgegenstände, der Geld- und Wertzeichenfälschung usw

<sup>78</sup> Vgl. hierzu und zum Folgenden *Rath* DRiZ 2016, 292 (293).

<sup>79</sup> Hierzu und zum Folgenden s. BGH NStZ 1995, 516 (517); *Fischer/Maul* NStZ 1992, 7 (8).

<sup>80</sup> BGH NStZ 2001, 553 (554).

<sup>81</sup> BGH NStZ 2000, 269 (271).

<sup>82</sup> BGH NStZ 2000, 269 (271).

<sup>83</sup> EGMR JR 2015, 81 Rn. 48.

<sup>84</sup> BGH NJW 2001, 2981; NStZ 1992, 488.

<sup>85</sup> Vgl. dazu *Mosbacher* JuS 2016, 127.