Recht

Rezension

Thomas-Gabriel Rüdiger/ Petra Saskia Bayerl (Hrsg.): *Cyberkriminologie. Kriminologie für das digitale Zeitalter.* Wiesbaden 2020: Springer VS. 755 Seiten, 54,99 Euro

Cyberkriminologie

Die Kriminologie ist seit jeher ein interdisziplinäres Feld, das sich aus zahlreichen Bezugswissenschaften zusammensetzt. Nur folgerichtig erscheint vor diesem Hintergrund, dass Thomas-Gabriel Rüdiger und Petra Saskia Bayerl sich im Rahmen der Herausgeberschaft des Sammelbandes bei den insgesamt 28 Beiträgen einer breiten Autorenschaft aus der Rechtswissenschaft, der Psychologie, der Soziologie und Politologie sowie weiteren – auch berufspraxisnahen – Wirkbereichen eines soliden interdisziplinären Fundaments versichert haben.

So vielgestaltig die Bezugspunkte der Internetkriminalität in einer vollständig digitalisierten Gesellschaft sind, so gewaltig erscheint die Herausforderung ihrer Fassung in einem einzigen Buch. Dies kann auch bei einem Umfang von mehr als 700 Seiten nur eklektisch und ohne Anspruch auf Vollständigkeit gelingen, sodass die nur lose thematische Klammerung in die Abschnitte „Grundlagen der Cyberkriminologie", „Phänomenologie von Kriminalität im digitalen Raum" sowie „Normenkontrolle und digitale Polizeiarbeit" zunächst unscharf und vage bleiben muss. Jedoch wird gleich im ersten Beitrag durch die Herausgeberin und den Herausgeber (S. 3 ff.) ein plausibler roter Faden durch Aufbau und Chronologie der nachfolgenden Beiträge gesponnen, welche im Rahmen dieser Rezension freilich nicht alle erwähnt und besprochen werden können. Vielmehr erfolgt eine Auswahl, die insbesondere die Beiträge zu den „Grundlagen der Cyberkriminologie" fokussiert.

Klug wirft Holger Plank in seiner Betrachtung aus der Perspektive einer „Gesamten Strafrechtswissenschaft" die eigentlich schon mit dem Titel des Sammelbandes evozierte Frage nach der Kontur des Begriffs der „Cyberkriminologie" auf. Hebt der Autor die Bedeutung und (empirische) Rolle der Kriminologie im Konzert der „Gesamten Strafrechtswissenschaft" in der Diktion v. Liszts auch hervor, so wird auch eine kritische Distanzierung von der Terminologie der „Cyberkriminologie" allein dadurch deutlich, dass sie nach Auffassung Planks derzeit die „Verbrechenswirklichkeit" „noch gar nicht ausreichend oder gar als ontologische Entität" konturiere. Zutreffend weist er darauf hin, dass allein die terminologische Institutionalisierung einer Subkategorie der Kriminologie wenig leistet, solange ihr eine unklare Phänomenologie gegenübersteht. Insoweit bleibt sie zum Gutteil vage Worthülse.

Hoheisel-Gruler erweitert in seinem sehr lesenswerten Beitrag die in der Politik oft verwandte und – wie der Autor selbst bemerkt – banale Phrase „Das Internet ist kein rechtsfreier Raum" umsichtig zu dem Titel *Der digitale Raum ist kein (grund-)rechtsfreier Raum*. Er weist auf die wechselseitigen Dynamiken der Digitalisierung hin, wonach die digitale Welt nicht nur als Adaption der analogen Lebensumgebung begriffen werden kann. Dies erscheint auch mit Blick auf die weiteren spezifizierenden Beiträge des Sammelbandes wichtig, da hierauf das Postulat einer eigenständigen Disziplin der „Cyberkriminologie" möglicherweise gestützt werden kann. Korrekt legt der Autor die verfassungsrechtlichen Grundlagen in

wesentlichen Zügen dar und zeigt das Spannungsfeld miteinander in Konflikt tretender verfassungsrechtlicher Belange etwa anhand der Wechselwirkungslehre auf. Auf dieser Grundlage prüft er Befugniserweiterungen in der polizeilichen Ermittlungsarbeit (z. B. Onlinedurchsuchungen) im digitalen Raum, ehe sich Hoheisel-Gruler der kriminologischen These der – nach Ansicht des Rezensenten noch vagen und nicht in allen Punkten überzeugenden – Übertragung der klassischen Broken-Windows-Theorie auf das Internet zuwendet. Hier wäre ein kritischerer Blick derart möglich gewesen, dass der These eines beobachtbaren kontrollfreien Verrohungspfuhls im Internet die Phänomenologie einer spätestens durch das Netzwerkdurchsetzungsgesetz (NetzDG) umfassenden Lösch-Compliance in großen sozialen Netzwerken gegenübersteht, welche auch angesichts der Zahlen entfernter Inhalte eher Indizien für ein Overblocking denn für Normkontrollverlust liefert. Die nun vorgesehenen, weitgehend automatischen Ausleitungen solcher Fälle an das BKA § 3a NetzDG hätten in diesem Kontext doch zumindest Erwähnung finden müssen. Immerhin erfolgt ein Überblick zum Netzwerkdurchsetzungsgesetz de lege lata in sehr ausgewogener Weise in einem anderen Abschnitt (8.), freilich nicht mehr zuvörderst im Kontext des Broken-Web-Ansatzes.

Zur Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime äußern sich Edith Huber und Bettina Pospisil, wobei in dem ebenso betitelten Beitrag zunächst die differenzierende Taxonomie von Cybercrime in drei Varianten („core cybercrime", „non-cyberspecific cybercrime" und „Verschleierung der Identität") gewinnbringend erscheint. Bedenken einer systematischen Stringenz und Vollständigkeit bei der deskriptiven Darstellung werden mit einiger Berechtigung aufgeworfen. Dezidiert und umfassend werden dann die Begriffe des Hellfeldes und des Dunkelfeldes erklärt und die Methoden der Erfassung (insbesondere des Hellfeldes) dargestellt, wobei die Problematik und die Herausforderungen hinsichtlich des Dunkelfeldes deutlich werden. Die Darstellung von Phänomenologie und Kasuistik erfolgt mit Fokus auf den österreichischen Forschungs- und Wirkbereich der Autorinnen.

Dirk Kunze befasst sich in seinem Beitrag *Strafverfolgung digital* mit der – auch anlassunabhängigen – Ermittlung und Verfolgung von Straftaten im Cyberbereich sowie dem Erkennen und Abwehren von Gefahren im Internet. Der Autor rekurriert dabei auch auf den Erfahrungsfundus aus dem Aufbau und der Leitung des Ermittlungsdezernats des Cybercrime-Kompetenzzentrums des LKA NRW und der zentralen Internetrecherche. Schwerpunktbereiche der Internetfahndung, namentlich 1.) der personenzentrische Ansatz, 2.) der sachbezogene Ansatz, 3.) die Unterstützungsleistungen und 4.) Ermittlungskommissionen werden dargestellt, ehe – z. T. korrespondierend mit dem anderweitigen Beitrag von Henkel (S. 175 ff.) – Kriminalitätsformen im Darknet und darüber hinaus im sogenannten „Surfaceweb" in den Blick genommen werden, wobei eher deskriptiv Kasuistik, etwa der Amoklauf eines 18-Jährigen in München am 22. Juli 2016 sowie der Waffenhandel, erwähnt wird. Erkenntnisgewinn bringt vor allem das ausführliche vierte Kapitel „Ohnmacht im Netz?", welches über die Implikation des Titels hinaus zahlreiche Kriminalitätsbereiche (illegale Handelsplattformen, Hasskriminalität, Cybergrooming, Kinderpornografie) im Hinblick auf Herausforderungen der Ermittlungs- und Verfolgungsarbeit sowie aktuelle praktische und legislative Ansätze (Gesetzentwurf zur Bekämpfung von illegalen Marktplätzen) überblickshaft beleuchtet.

In dem Beitrag *Defensible Digital Space* verfolgen Cindy Ehlert und Thomas-Gabriel Rüdiger den Ansatz, eine Raumtheorie des Architekten und Stadtplaners Oscar Newman zur Kriminalprävention und Nachbarschaftssicherheit für den Onlinebereich zu adaptieren. Dabei bleiben die Betrachtungen allerdings zuweilen an der Oberfläche, Problemstellungen einer Übertragbarkeit werden zwar benannt, dann in der weiteren Abhandlung jedoch nur noch z. T. wieder aufgegriffen. Allein die „Interaktion der Menschen miteinander" als Bindeglied bzw. gemeinsame Basis für die Entstehung von Kriminalität in bestimmten Räumen erscheint limitiert angesichts der erheblichen strukturellen Unterschiede, welche auch bei den von der Autorin und dem Autor gewählten Beispielen Zweifel evozieren. Dies gilt etwa für die Benennung des „unerwünschten Zusendens pornografischer Medien" (welche gegenüber erwachsenen Personen schon nicht per se strafbar ist), die in Newmans relevantem „physischem" Delinquenzbereich enger Wohnräume mit vielen Menschen schon kaum eine Entsprechung findet. Auch wird gerade bei den sozialen Medien, welche in dem Beitrag in den Fokus gestellt werden, zu wenig berücksichtigt, dass Medienzuwendungsmotivationen der Nutzerschaft ganz andere sind als die oftmals sozial determinierte, unfreie Nutzung eines bestimmten Wohnraums. Auch soziopsychologische, kriminalitätsfördernde Ursachen gestalten sich im Bereich physisch-körperhafter Beengung und Konzentration vieler menschlicher Individuen anders als bei dem rein kommunikativen Zusammentreffen und Interagieren im Internet. Vor diesem Hintergrund bleibt das Analogon „Facebook" – „Wohnblock" fragwürdig. Schließlich entfernen sich dann auch die vorgeschlagenen Mechanismen wie „Counter Speech" oder im Jugendschutz „Safety-by-Design" von dem eigentlichen Ansatz Newmans, der zuvörderst auf die Evozierung eines „Ownership"- und Eigenverantwortungsgefühls bei den Bewohnerinnen und Bewohnern abstellte. Dies findet in den Praxisvorschlägen nicht immer eine Entsprechung, sodass gerade der Mehrwert des Rückgriffs auf die klassische Raumtheorie Newmans weiter infrage steht. Gleichwohl ist das Wagnis der Kontextualisierung klassischer kriminologischer Ansätze zu „Cyber"-Phänomenologien grundsätzlich verdienstvoll und diskussionswürdig.

Die im zweiten Abschnitt des Sammelbandes vielfältig behandelte „Phänomenologie von Kriminalität im digitalen Raum" kann im vorgegebenen Rahmen nur ganz überblickhaft dargestellt werden. Einen Schwerpunkt bildet sicher die Betrachtung des „Cyberterrorismus" in den Beiträgen von Holger Nitsch (S. 193 ff.) sowie von Enghofer, Müller und Parrino

(S. 217 ff.). Daneben liefert Christian Thiels Beitrag *Liebesschwindel im Cyberspace* (S. 241 ff.) interessante Einblicke in das Phänomen des sogenannten „Romantikbetrugs", der freilich nicht soziophilosophisch in Bezug auf die häufige Chronologie menschlicher Partnerschaften, sondern ausschließlich mit Blick auf Betrugskriminalität gemeint ist. *Hate Speech in der Computerspielkultur* (Sonja Gabriel, S. 269 ff.) wird ebenso delikts- und phänomenologiespezifisch beleuchtet wie *Cyberangriffe gegen private Internetnutzer*innen* (Dreißigacker/von Skarczinski/Bergmann/Wollinger, S. 319 ff.). Neben weiteren lesenswerten Beiträgen (deren namentliche Nennung und ausführlichere Besprechung nur wegen des beschränkten Rezensionsumfangs nicht möglich ist) liefern Stelzmann, Amelung und Kuhle interessante Einblicke in *Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland* (S. 475 ff.)

Im letzten Teil des Sammelbandes werden Mechanismen der Normenkontrolle sowie die Rolle bzw. Möglichkeiten digitaler Polizeiarbeit behandelt. Dabei wird neben den Mitteln praktischer Ermittlungsarbeit (vgl. etwa Povalej/Volkmann: *GIS und Geoinformatik bei der Polizei. Chancen und Potenziale für Ermittlungen* (S. 685 ff.) sowie Konstanze Marx (S. 707 ff.) zu automatischen Verfahren bei der Detektion von Hate Speech) in mehreren Beiträgen eine grundsätzlichere kriminologische Perspektive eingenommen, welche nicht zwingend nur den Bereich der Normenkontrolle und der Polizeiarbeit betrifft. Exemplarisch zu benennen ist der Beitrag von Piasecki und Dienstbühl (S. 489 ff.), die sich mit dem generellen Sicherheitsempfinden der Nutzer in sozialen Netzwerken auseinandersetzen. Allerdings erscheint fraglich und wäre weiter zu untersuchen, inwieweit die nur von einem sehr geringen Teil der Internetnutzerschaft betroffenen, in dem Beitrag beleuchteten Delinquenzbereiche (Cybergrooming, Romance-Scamming) und singuläre Ausnahmeereignisse wie die Blue Whale Challenge geeignet sind, Rückschlüsse auf ein repräsentatives Sicherheitsgefühl im Gesamten ziehen zu können. Hier scheinen Deliktsbereiche mit einer breiteren potenziellen Betroffenheit von Nutzerinnen und Nutzern (Datenschutzdelikte wie Ausspähung, Phishing etc.) aus Sicht des Rezensenten näherliegende Parameter und Ansatzpunkte für ein ohnehin schwer empirisch zu fassendes Sicherheitsgefühl einer nicht weiter differenzierten Nutzerschaft zu sein.

Insgesamt kann der Sammelband als gelungenes Kompendium kriminologischer sowie auch rechtswissenschaftlich und kriminalistisch orientierter Beiträge im Kontext der Internetdelinquenz angesehen werden. Naturgemäß ist bei 28 Einzelbeiträgen die Niveauvarianz hinsichtlich Wissenschaftlichkeit, Struktur und Aufbau sowie Sprachstil und Duktus breit. Dies zeigt sich etwa an dem einerseits aufgrund des Ich-Erzählstils an den Duktus studentischer Abschlussarbeiten erinnernden Beitrag *Digitaler Vigilantismus*, der auch inhaltlich Grundlagen über die Strafbarkeit klassischer vigilantistischer Handlungen wie Bildnisveröffentlichungen (vgl. §§ 22, 23 KUG oder auch § 201a StGB) oder Spruchpraxis der Bundesprüfstelle zur Prangerwirkung von Internetveröffentlichungen zu wenig berücksichtigt. Andererseits zeichnet sich z. B. Planks nachgerade rechtsphilosophische Abhandlung zur Kontur des Begriffs „Cyberkriminologie" durch eine enorme gedankliche Komplexität und Stringenz, ein exzellentes Sprachniveau sowie die jeder guten ontologischen Betrachtung förderliche Perspektivenbreite aus.

Wer sich aus dem klassischen Wissenschaftsfeld der Kriminologie – wie auch der Kriminalistik und (Straf-)Rechtswissenschaft – heraus mit Ursachen der Internetdelinquenz sowie praktischen Ansätzen der Ermittlungsarbeit und Gefahrenabwehr befasst, dürfte an dem von Thomas-Gabriel Rüdiger und Petra Saskia Bayerl herausgegebenen Werk kaum vorbeikommen. Aufgrund des Umfangs und der Vielfalt der – ohne Anspruch auf Vollständigkeit – behandelten Aspekte kommt dem Buch nachgerade ein enzyklopädischer Charakter zu, der – in der Diktion v. Liszts in der „Gesamten Strafrechtswissenschaft" – ein Gewinn ist. Dem Werk ist weite Verbreitung zu wünschen.

Prof. Dr. Marc Liesching