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

Klaus Malek/Andreas Popp, Strafsachen im Internet, C. F. Müller, Heidelberg, 2. Aufl. 2015, 161 S., € 44,99.

Den geradezu unbegrenzten Möglichkeiten weltweiter Kommunikation und Information, die das Internet bietet, stehen die ebenso unbegrenzten Möglichkeiten gegenüber, das Internet zu strafwürdigen Zwecken zu missbrauchen. Sei es, weil das Internet als Tatmittel zu kriminellen Zwecken genutzt wird oder sei es, weil es den „Tatort" bildet. Dass dies tagtäglich auch mannigfach geschieht, bedarf wohl keiner näheren Erläuterung. Jedoch ist für viele Strafverteidiger die Welt des World Wide Web und der weiteren Internetdienste jenseits der eigenen Nutzung für berufliche und private Zwecke noch weitgehend als terra incognita zu bezeichnen. Dies ist misslich, nicht nur weil die Kenntnis zumindest der grundlegenden technischen Zusammenhänge für eine adäquate Verteidigung in Fällen mit Internetbezug unabdingbar ist, sondern auch weil sich hier rechtliche Besonderheiten ergeben, die es im Rahmen der Verteidigung zu berücksichtigen gilt. Dabei stellt sich die Materie der Internetkriminalität noch als junges Teilgebiet des Strafrechts dar, in dem viele Streitigkeiten bestehen und oftmals eine gefestigte Rechtsprechung (noch) nicht gegeben ist. Um dem Strafverteidiger hier Abhilfe zu schaffen und einen ersten Einblick und Einstieg in diese Spezialmaterie zu ermöglichen, hat *Klaus Malek* die zweite Auflage seines Handbuchs vorgelegt. Als Coautor konnte er *Andreas Popp* gewinnen.

Das Handbuch richtet sich in erster Linie an Strafverteidiger. Es soll dabei sowohl als Einstieg in die Spezialmaterie, als auch als Nachschlagewerk dienen. Es kann aber ebenso von Praktikern in der Justiz als solches verwandt werden. Als Lehrbuch, etwa für Schwerpunktstudenten, ist es weder gedacht noch zu empfehlen. Schon der für die Praxis begrüßenswert knappe Umfang kann dies nicht leisten.

Inhaltlich ist das Handbuch in drei Teile gegliedert. Der erste Teil (Rn. 1-53) beinhaltet neben einer kurzen Einführung die notwendigen Grundlagen zum Verständnis des Internets. Zunächst stellen die *Autoren* fest, dass eine gesetzestechnische Spezialmaterie des Internetstrafrechts nicht existiere. Vielmehr seien die strafrechtlichen Vorschriften des Kern- und Nebenstrafrechts auch auf Sachverhalte mit Internetbezug anzuwenden, wobei dessen Besonderheiten zu beachten seien. Im Anschluss wird ein kurzer Abriss der Geschichte des Internets gegeben (Rn. 12-20). Sodann werden dessen technische Grundlagen erläutert (Rn. 21-27). Hierbei sei insbesondere zu beachten, dass das Internet keine zentral betriebene hierarchische Datenbank sei, sondern sich vielmehr als weltweiter Netzwerkverbund der angeschlossenen Rechner darstelle, in den jeder Rechner gleichberechtigt einbezogen sei. Innerhalb dieses Verbundes tauschten die einzelnen Rechner nach einem bestimmten Schema (Verbindungsaufbau, Anfrage, Antwort, Verbindungsabbau) Daten aus. Die Versendung der Daten erfolge dabei nicht als Ganzes, sondern die Informationen werden in kleinere Pakete aufgeteilt und über das Netzwerk versandt. Jedes Paket werde auf einem individuellen Weg durch das Netzwerk an den Zielrechner übertragen. Am Zielort werden die Pakete dann auf Vollständigkeit überprüft und in der richtigen Reihenfolge wieder zusammengesetzt. Auf diese Weise könnten auch größere Datenmengen in kurzer Zeit schnell versandt und empfangen werden. Damit die Datenaufteilung und -zusammensetzung korrekt funktioniere, befolgten alle Rechner ein einheitliches Schema, das sogenannte TCP-Protokoll. Die Versendung und die Routenwahl der einzelnen Pakete erfolge ebenfalls nach einem einheitlichen Schema, dem sogenannten IP-Protokoll. Neben dieser Erläuterung des Begriffs des TCP/IP-Protokolls erklären *Malek* und *Popp* auch weitere Begriffe wie beispielsweise die verschiedenen Dienste des Internets (Rn. 28-46), darunter das World Wide Web (Rn. 29 ff.), E-Mail (Rn. 33 ff.) und Internet-Relay Chat (Rn. 41 f.).

Der erste Teil schließt mit einer Erläuterung der am Internet Beteiligten (Rn. 47-53). Diese untergliederten sich nach dem Telemediengesetz (TMG) grundsätzlich in zwei Kategorien: die Anbieter (Provider) und die Nutzer (User). Während Anbieter gem. § 2 Nr. 1 TMG jede natürliche oder juristische Person sei, die eigene oder fremde Telemedien zur Nutzung bereithalte oder den Zugang zur Nutzung vermittele, sei Nutzer nach § 2 Nr. 3 TMG jede natürliche oder juristische Person, die Telemedien nutze, insbesondere um Informationen zu erlangen oder zugänglich zu machen. Die Anbieter untergliederten sich dabei in die Content-Provider (Rn. 49), die Inhalte anbieten, die Service-Provider (Rn. 50), die eine Vielzahl unterschiedlicher Services zu Verfügung stellten wie beispielsweise den Zugang zum Netz, die Bereitstellung von Festplattenkapazitäten zum Betreiben einer Homepage (Host-Provider) oder zur Speicherung von Daten (Cloud), sowie in die Access-Provider (Rn. 51), die lediglich den Zugang zum Netz vermittelten. Diese Aufteilung wird im späteren Verlauf aufgegriffen und zur Grundlage der Zuordnung von strafrechtlichen Verantwortlichkeiten gemacht. Es gelingt den *Autoren* dabei, die zum Teil höchst komplexen technischen Zusammenhänge und die kryptischen Fachbegriffe in einer dem technischen Laien klar verständlichen Form zu erläutern, ohne sich unnötig in Details zu verrennen.

Im zweiten Teil (Rn. 54-417) gehen die *Autoren* auf das materielle Internetstrafrecht ein. Dabei werden zunächst in einem Allgemeinen Teil (Rn. 54-146) grundlegende Fragen zu Zuständigkeiten der deutschen Strafgewalt oder die Verantwortlichkeiten der am Internet Beteiligten behandelt. In einem Besonderen Teil (Rn. 147-417) folgen dann Erläuterungen zu einzelnen Tatbeständen des Kern- und Nebenstrafrechts. Die Darstellungen im gesamten zweiten Teil enthalten jeweils knappe grundlegende Informationen und widmen sich sodann den internetspezifischen Besonderheiten der Regelungen.

Im Allgemeinen Teil setzen sich die *Autoren* zunächst mit der Zuständigkeit der deutschen Strafjustiz auseinander (Rn. 54-68). Hier sei das gem. der §§ 3, 9 StGB geltende Territorialitätsprinzip zu beachten. Doch gerade die Bestimmung des Tatorts könne sich im Rahmen von Internetsachverhalten problematisch gestalten. Während sich bei Erfolgs- und konkreten Gefährdungsdelikten keine Besonderheiten ergäben, sei die Bestimmung des Tatorts bei abstrakten Ge-

fährdungsdelikten hoch umstritten (Rn. 63 ff.). Einerseits werde angenommen, ein abstraktes Gefährdungsdelikt habe keinen Erfolg und somit auch keinen Erfolgsort, sodass als Tatort lediglich der Handlungsort in Frage komme. Demgegenüber werde aber vertreten, dass ein Erfolgsort bei abstrakten Gefährdungsdelikten überall dort gegeben sei, wo sich die abstrakte Gefahr realisieren könne. Dies umfasse wegen der weltweiten Zugänglichkeit des Internets auch deutsches Hoheitsgebiet, sodass eine Art Allzuständigkeit der Deutschen Justiz die Folge wäre. Dieses Ergebnis werde von einigen Autoren teleologisch mit dem Bezug auf ein finales Interesse reduziert. *Malek* und *Popp* erwähnen in diesem Zusammenhang auch das Urteil des BGH v. 12.12.2000, der in Bezug auf § 130 StGB von einem abstrakt-konkreten Gefährdungsdelikt sprach. Eine endgültige Entscheidung bezüglich aller abstrakten Gefährdungsdelikte sei hiermit jedoch nicht erfolgt, sodass der Verteidigung bei anderen Tatbeständen noch Raum zur Argumentation verbleibe. Die bestehende Rechtslage bezeichnen sie als bedenklich, was aber durch die praktisch fehlende Durchsetzbarkeit des deutschen Strafanspruchs relativiert werde (Rn. 68).

Im Folgenden (Rn. 69-106) wird die Frage der Verantwortlichkeiten der am Internet Beteiligten bearbeitet. Hier wird festgestellt, dass für die Frage der Verantwortlichkeiten grundsätzlich der Allgemeine Teil des StGB bestimmend sei. Dieser werde ergänzt durch die §§ 7-10 TMG und den Rundfunkstaatsvertrag (RStV). Fraglich sei jedoch, in welchem Verhältnis die Regelungen stünden. Die *Autoren* lehnen die sog. Integrationslösung, wonach die Tatbestandsmerkmale der §§ 7 ff. TMG in die Tatbestände der allgemeinen Regelungen eingefügt werden, ab. Sie votieren vielmehr für die als Vorfilterlösung bezeichnete Ansicht, nach der zunächst die Verantwortlichkeit des Betroffenen gem. der §§ 7 ff. TMG zu prüfen ist. Erst wenn diese vorliege könne eine strafrechtliche Verantwortlichkeit in Betracht kommen, die sich nach den allgemeinen Regelungen bestimme (Rn. 74). Auf dieser Grundlage wird nunmehr die Verantwortlichkeit der Beteiligten im Detail betrachtet (Rn. 75-106). Die *Autoren* nehmen an, dass sich ergebe, dass ein Provider für die von ihm angebotenen eigenen Inhalte strafrechtlich verantwortlich sei. Dabei wird näherer betrachtet, wann ein Inhalt als „eigener" zu qualifizieren ist. Nach *Popp* sollen dies grundsätzlich nur die vom Anbieter selbst hergestellten Inhalte sein, es sei denn, dass sich der Anbieter einen fremden Inhalt durch eindeutige Identifizierung zu eigen mache oder der fremden Aussage durch Übernahme und bewusste Zusammenstellung mit anderen Inhalten einen neuen, eigenständigen Gesamtinhalt gebe, der über die Summe der Einzelteile hinausgehe (Rn. 80). Für die Praxis raten die *Autoren* ernsthafte Distanzerklärungen (Disclaimer) für fremde Inhalte an.

Problematisch sei auch, ob sich jemand durch das Setzen eines sog. Hyperlinks (Verweisung auf eine Information eines Dritten) die verlinkte Information zu eigen mache (Rn. 83). Die *Autoren* erteilen der Ansicht, eine solche Verlinkung führe automatisch zur Zurechnung der Information zum Linksetzenden, eine Absage. Hierdurch werde die Meinungsfreiheit verletzt und ein Widerspruch zu den im Presserecht entwickelten Grundsätzen heraufbeschworen. Vielmehr seien die oben genannten Grundsätze nach *Popp* auch hier anzuwenden. Aufgrund des Umstandes, dass der Linksetzende aber einen fremden Inhalt sucht und ihn gezielt anderen Nutzern zur Verfügung stellt, seien an die Klassifizierung als eigene Aussage geringere Anforderungen zu stellen.

Für fremde Inhalte besteht nach *Malek/Popp* grundsätzlich keine strafrechtliche Verantwortlichkeit (Rn. 86-106). Nach dem Privileg des § 10 Nr. 1 TMG seien Provider für Informationen, die über einen durch sie vermittelten Zugang oder die über ihre Kommunikationsnetze übermittelt werden, nicht verantwortlich. Dies gelte jedoch nur, soweit der Anbieter keine Kenntnis von der rechtswidrigen Handlung oder Information habe. Es gelte ein enger Maßstab der Kenntnis, der die positive Kenntnis der Web-Adresse und ihres rechtswidrigen Inhalts erfordere. Erst bei einem solchen Wissensstand sei der Provider zum Tätigwerden verpflichtet (Rn. 88).

Im Übrigen wendet sich der Allgemeine Teil der materiell strafrechtlichen Bearbeitung klassischen Bereichen des Allgemeinen Strafrechts zu, wie der Abgrenzung von Tun und Unterlassen (Rn. 107-110), dem Bestehen von Garantenpflichten (Rn. 111-124), der Abgrenzung von Täterschaft und Teilnahme (Rn. 125-138) oder Vorsatz und Fahrlässigkeit (Rn. 139-146). Die Ausführungen sind sämtlich kurz und prägnant gehalten und beschränken sich weitgehend auf die besonderen internettypischen Problemstellungen. Hierbei werden bestehende Streitstände knapp dargestellt, zum Teil nur die wesentlichen Hauptargumente genannt.

Zu Beginn des Besonderen Teils des zweiten Teils wiederholen die *Autoren* den Umstand, dass das Gesetz keine internetspezifischen Delikte kenne (Rn. 147). Vielmehr seien internetspezifische Verhaltensweisen zu identifizieren und den klassischen Tatbeständen des besonderen Strafrechts zuzuordnen. Die weitere Darstellung der einzelnen Tatbestände ist nach dem thematischen Bezug gegliedert. Zunächst werden Straftaten mit wirtschaftlichem Bezug behandelt (Rn. 148-259), sodann urheberrechtliche Straftaten (Rn. 260-311), Straftaten gegen persönliche Rechte und Geheimnisse (Rn. 312-317), inhaltsbezogene Delikte (Rn. 318-400), Delikte gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen (Rn. 401-412) und exhibitionistische Handlungen (Rn. 413-415) sowie Prostitution (Rn. 416-417).

Bereits im Rahmen der Straftaten mit wirtschaftlichem Bezug zeigt sich die ganze Bandbreite des internetspezifischen Strafrechts. Mit dem Ausspähen von Daten nach § 202a StGB, der Datenveränderung gem. § 303a StGB, der Fälschung beweiserheblicher Daten gem. § 269 StGB, Betrug gem. § 263 StGB, Computerbetrug nach § 263a StGB, der Unerlaubten Veranstaltung eines Glückspiels nach § 284 StGB und einigen weiteren Tatbeständen wenden sich die *Autoren* Bereichen des besonderen Strafrechts zu, die unterschiedlicher kaum sein könnten. Die Darstellung erfolgt in Form einer recht knapp gehaltenen Kurzkommentierung der jeweiligen Vorschrift, wobei immer auch auf die internetspezifischen Besonderheiten Bezug genommen und diese dann ausführlich dargestellt werden.

Beispielhaft seien die Ausführungen zu § 202a StGB (Rn. 147-173) erwähnt. Hiernach ist das unbefugte Sichverschaffen von Daten unter Überwindung von Zugangssiche-

rungen unter Strafe gestellt. Die *Autoren* erläutern die einzelnen Tatbestandsmerkmale und problematisieren, ob das weit verbreitete Verschlüsseln von Daten auch als Zugangssicherung i.S.d. § 202a StGB zu qualifizieren sei (Rn. 159). Denn die Verschlüsselung diene nicht der Verhinderung des Zugriffs auf die Daten, sondern einzig der Verhinderung der unbefugten Kenntnisnahme des Bedeutungsgehalts der Daten. Der diesbezüglich h.M., die die Verschlüsselung als Zugriffssicherung annimmt, stehen die *Autoren* höchst skeptisch gegenüber. Auch Fälle des Hacking sowie der Einsatz von Trojanern (wobei zwischen Sniffer, Keylogger und Backdoor-Trojanern unterschieden wird) werden vor dem Hintergrund des § 202a StGB bewertet (Rn. 161-164). Jede dieser Varianten sei unter den Tatbestand des § 202a StGB zu subsumieren. Gleiches sei bei einer Brute Force-Attack (Trial and error-Verfahren zur Ermittlung eines Passworts, Rn. 163) sowie beim Spoofing (Vortäuschen einer falschen Identität, Rn. 165) der Fall. Anders sei aber die Installation sog. Dialer-Programme zu bewerten. Hierbei wird ein Programm auf einem Rechner installiert, welches dann nicht die normalerweise gebräuchliche Verbindung zum Internet herstellt, sondern eine hoch gebührenpflichtige Internetverbindung. Es werde hier lediglich die Art der Verbindung ausgetauscht, ein Zugriff auf die Daten des Betroffenen erfolge im Regelfall nicht (Rn. 166). Aus dem gleichen Grund sei die Installation eines Virusprogramms oder anderer Schadsoftware, die lediglich Daten zerstören, nicht unter § 202a StGB zu subsumieren. Insofern komme aber § 303a StGB in Betracht.

Auch im Rahmen der Bearbeitung der folgenden Tatbestände nehmen sich die *Autoren* praxisrelevanter Fallgestaltungen mit Internetbezug an. So gehen sie etwa der Frage nach, ob § 202c Abs. 1 Nr. 2 StGB erfüllt ist, wenn der Täter ein Programm herstellt oder erwirbt, dass sowohl zu legalen, als auch zu illegalen Zwecken eingesetzt werden kann (sog. Dual Use-Programme). Entgegen *Fischer*, der auf den wesentlichen Zweck des Programmes abzielt, votieren *Malek/Popp* dazu, Dual Use-Programme gänzlich aus dem Anwendungsbereich des § 202c StGB auszunehmen (Rn. 175). Auch in Bezug auf die Strafbarkeit nach § 303a StGB beim Aufheben einer Sim-Lock-Sperre eines Mobiltelefons verlangen die *Autoren* die Straflosigkeit des Betroffenen, wenn er zuvor das Mobiltelefon erworben hat und hiermit die Verfügungsgewalt über die Daten auf ihn übergegangen ist. Die Gegenansicht, die eine Strafbarkeit gem. § 303a StGB annehme, sanktioniere im Ergebnis zivilrechtliche Vertragsverletzungen durch das Strafrecht, was dem Normzweck nicht entspreche (Rn. 185).

Der Stil der Kurzkommentierung zieht sich durch den gesamten Besonderen Teil, jeweils mit dem erwähnten Internetbezug. Die Darstellungen orientieren sich an den in der Praxis häufig auftretenden Fallgestaltungen und Problemstellungen. Die zum Teil recht kurzen Ausführungen werden immer durch weiterführende Literaturnachweise ergänzt, sodass der Leser für eine vertiefte Auseinandersetzung mit einem Spezialproblem ausreichend Rechercheansätze zur Verfügung gestellt bekommt.

Bedauerlich ist, dass die *Autoren* das 49. Strafrechtsänderungsgesetz, welches im Januar 2015 in Kraft trat und u.a. der Umsetzung der Richtlinie 2011/93/EU vom 13.12.2011 diente, wegen des Termins der Drucklegung nicht mehr berücksichtigen konnten. Es enthält Änderungen von Tatbeständen, die im Rahmen der Bearbeitung von *Malek* und *Popp* sicherlich Auswirkungen haben werden, etwa in Bezug auf die Delikte gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen (vgl. nur Rn. 319, 330, 353). Diese Neuerungen werden erst in der sicher zu erwartenden dritten Auflage berücksichtigt werden können.

Ebenfalls keine Aufnahme in den Bearbeitungskatalog haben die Tatbestände gefunden, die weithin als Teil des „Terrorismusstrafrechts" bezeichnet werden. Hierzu gehören u.a. die §§ 89a, 89b StGB oder die §§ 129a, 129b StGB. Dabei kommt etwa die Unterstützung einer terroristischen Vereinigung gem. § 129a Abs. 5 StGB durch Propagandawerbung oder Spendensammlungen im Internet als mögliche Tatvariante in Betracht. Daneben kann die Unterweisung bzw. das Unterweisenlassen im Umgang mit Sprengstoff oder Waffen gem. § 89a Abs. 1 Nr. 1 StGB z.B. durch das Einstellen oder Konsumieren von Videodateien in das bzw. über das Internet geschehen (z.B. build your own bomb-Video). Auch wenn vor dem Hintergrund der Bedeutung des Internets für die modernen Erscheinungsformen extremistisch motivierter Straftaten eine Behandlung wünschenswert gewesen wäre, erscheint der Verzicht hierauf jedoch als vertretbar, da insoweit die Problemstellungen zum Teil im Rahmen anderer Tatbestände aufgegriffen wurden (z.B. bei § 130a StGB, dort Rn. 390 ff.), zum Teil sich durch den Internetbezug keine oder nur geringe Abweichungen von Fällen ohne Internetbezug ergeben und weil insoweit ausreichend Spezialliteratur vorhanden ist.

Im dritten und letzten Teil (Rn. 418-485) nehmen sich die *Autoren* den strafprozessualen Maßnahmen an, die in Fällen mit Internetbezug relevant werden können. Ebenso werden Ermittlungsmaßnahmen besprochen, die einen Internetbezug aufweisen.

Zunächst wird konstatiert, dass die verdachtsunabhängige Recherche (virtuelle Streifenfahrt) durch die Ermittlungsgeneralklausel der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO gedeckt sei. Entsprechendes gelte für das schlichte Mitlesen offener Chat-Dialoge sowie das Abonnement offener Mailing-Listen (Rn. 420). Problematischer hingegen sei der Fall, in dem Polizeibeamte unter einer fingierten digitalen Identität an Aktivitäten im Netz teilnehmen. Hierin könne man generell einen Eingriff in das Grundrecht der informationellen Selbstbestimmung sehen, der eine weitergehende Ermächtigungsgrundlage erfordere, die derzeit nicht bestehe (Rn. 421). Der insoweit vertretenen analogen Anwendung der Vorschriften über den Einsatz Verdeckter Ermittler stehen die *Autoren* skeptisch gegenüber. Die Diskussion sei jedoch durch die Entscheidung des BVerfG zur sog. „Online-Durchsuchung" praktisch entschärft worden. Denn das BVerfG habe entschieden, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung erst dann gegeben sei, wenn die staatliche Stelle das schutzwürdige Vertrauen des Betroffenen in die Identität und Motivation des Kommunikationspartners ausnutze, um persönliche Daten zu erheben, an die sie sonst nicht gelangen könnte. Gerade ein solches Vertrauen

sei in Bezug auf die Kommunikation im Internet wegen der dortigen völligen Anonymität und des Fehlens von Überprüfungsmechanismen nicht gegeben (Rn. 423).

Weiterhin widmen sich die *Autoren* dem Feld der inhaltlichen Überwachung und Aufzeichnung von internetgestützter Kommunikation (Rn. 432-447). Dabei wird z.B. die Kommunikation per E-Mail in fünf Phasen eingeteilt (Erstellung der E-Mail und dessen Entwurfsspeicherung als Phase 0, Absenden der Nachricht bis zum Eingang im Postfach des Empfängers als Phase 1, Speicherung im Postfach des Empfängers als Phase 2, das Abrufen durch den Empfänger als Phase 3 und die Speicherung auf dessen Rechner als Phase 4). Unstreitig seien die Phasen 0 und 4 nicht mehr als Telekommunikationsvorgang zu qualifizieren, so dass für den Zugriff der Ermittlungsbehörden die allgemeinen Regelungen der §§ 94 ff. StPO gelten (Rn. 443). Die Phasen 1 und 3 seien ebenso unproblematisch als Telekommunikationsvorgang anzusehen, sodass insoweit die besonderen Vorschriften zur Telekommunikationsüberwachung zur Anwendung gelangten, wenn die Behörden auf sie zugreifen wollten (Rn. 444). Strittig sei jedoch die Frage, wie die Phase 2 zu bewerten sei. Während die Rechtsprechung davon ausgehe, dass keine Telekommunikation stattfinde, weil die E-Mail an einem bestimmten Ort gespeichert sei und nicht übertragen werde, votieren *Malek/Popp* dafür, die Phasen 1 bis 3 als einheitlichen Kommunikationsvorgang anzusehen, sodass der Zugriff während der Phase 2 nur unter den engeren Voraussetzungen der §§ 100a ff. StPO erfolgen dürfe.

Das Handbuch endet mit einer Darstellung des Verfahrens zur Erhebung von Verkehrsdaten sowie zwei Exkursen, zum einen zum Einsatz sog. ISMI-Catcher, zum anderen zur Online-Durchsuchung.

Insgesamt stellt sich das Handbuch als kurze Einführung in die technischen Vorgänge und umfassende thematische Bearbeitung der rechtlichen Besonderheiten von strafrechtlichen Fallgestaltungen mit Internetbezug dar. Die Ausführungen sind immer klar verständlich und eingängig, erfordern aber ein rudimentäres technisches Vorwissen und gelegentlich die grobe Kenntnis bestimmter technischer Fachausdrücke. Es darf hierbei nicht übersehen werden, dass in der heutigen Zeit diese Kenntnisse von jedem durchschnittlichen Internetnutzer wohl erwartet werden können. Weiterhin sind die Ausführungen weitgehend knapp und prägnant gehalten. Zum Teil beschränken sie sich auf einzelne Kernpunkte von Problembereichen oder auf die Wiedergabe der Hauptargumentationslinien in Streitfällen. Dieser Umstand ist jedoch mit Blick auf den Zweck des Handbuchs und den Adressatenkreis nicht als Negativum zu werten. Vielmehr wird auf diese Weise das Problembewusstsein des Lesers für internettypische Fragestellungen geschärft, ohne das regelmäßig knappe Zeitbudget des Praktikers zu sehr einzuschränken. Aufgrund der Literaturnachweise und Verweisungen auf die Kommentarliteratur erhält der Leser stets Rechercheansätze, die eine weitere Vertiefung in einem Spezialproblem ermöglichen. Das Handbuch ist somit im Ergebnis als Einstiegsliteratur, aber auch als Kurznachschlagewerk für Praktiker, die sich mit strafrechtlichen Fallgestaltungen mit Internetbezug beschäftigen – oder in Zukunft beschäftigen wollen – uneingeschränkt zu empfehlen.

Akad. Rat a.Z. Dr. Markus Mavany, Trier