Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

4
K&R

24. Jahrgang April 2021 Seiten 221 – 296

dfv Mediengruppe · Frankfurt am Main

RA Stefan Hessel und Syndikusrechtsanwalt Carsten Klose, LL.M.*

Der Takedown-Request durch die Polizei – Eine neue Wunderwaffe gegen Fake Shops?

Kurz und Knapp

Die Polizei versucht dem Phänomen sogenannter Fake Shops im Internet seit einiger Zeit damit zu begegnen, dass sie Hosting-Anbieter um die Löschung der Shops bittet. Rechtsgrundlage und (Rechts-)Folgen dieser hier als „Takedown-Request" bezeichneten Vorgehensweise sind jedoch fraglich. Der Beitrag ordnet das Phänomen der Fake Shops zunächst aus Sicht der IT-Sicherheit ein, stellt daraufhin die bisherigen Bekämpfungsstrategien dar, um sodann eine rechtliche Beurteilung vorzunehmen und mögliche negative Rechtsfolgen für Hosting-Anbieter darzustellen.

I. Fake Shops als Teil der Underground Economy

Der Onlinehandel boomt und die Digitalisierung ist längst zum Wachstumstreiber geworden. Gleichzeitig hat auch die Kriminalität weitreichend Einzug in das Internet gehalten. Cybercrime ist seither auf dem Vormarsch und aus dem Netzwerk der Täter ist eine Underground Economy entstanden, in der unter anderem Handlungsanleitungen, Infrastrukturdienstleistungen und Serviceleistungen zur Geldwäsche für kriminelle Aktivitäten angeboten werden.[1] Ein Teil der kriminellen Aktivitäten, durch die der deutschen Wirtschaft jährlich Schäden von mehr als 100 Milliarden Euro entstehen,[2] entfällt dabei auf Fake Shops. Als Fake Shops werden Webseiten umschrieben, deren Betreiber bewusst und in betrügerischer Absicht den Eindruck eines normalen Onlineshops erwecken. In der Regel bieten die Täter auf der Webseite dann Waren zu verlockend günstigen Preisen an und der Kunde durchläuft einen normalen Bestellvorgang, an dessen Ende er zur Preisgabe von Kreditkartendaten oder zur Zahlung des Kaufpreises durch Überweisung per Vorkasse aufgefordert wird. Selbsterklärend ist, dass die bekannten Zahlungsdienstleister mit Käuferschutz entweder erst gar nicht angeboten werden oder eine Störung simuliert wird. Nach abgelaufener Lieferzeit muss der Kunde dann feststellen, dass er keine Ware erhält.

Welche Bedeutung Fake Shops genau in der Underground Economy haben und welche Gewinne die Täter erzielen, lässt sich mangels eindeutiger Ausweisung in den Statistiken der Landeskriminalämter und des Bundeskriminalamtes jedoch nicht in absoluten Zahlen beantworten.[3] Es ist jedoch davon auszugehen, dass Fake Shops für Cyberkriminelle nach wie vor ein profitables Geschäftsmodell darstellen. In einem im September 2019 vor dem LG Osnabrück verhandelten Fall ging es beispielsweise um nicht weniger als 811 Bestellungen im Umfang von 280 000 EUR.[4] Weiterhin ist davon auszugehen, dass sich der bereits vor einigen Jahren beschriebene Trend dynamisch fortgesetzt hat, wie etwa Warnungen vor Fake Shops und gefälschten Medikamenten im Zusammenhang mit der Corona-Pandemie zeigen.[5]

II. Fake Shops aus Sicht der Cybersicherheit

Das Aufsetzen und Betreiben von Fake Shops erfordert, wie viele andere Angriffe aus dem Bereich des Social Engineering, keine vertieften technischen Kenntnisse. Der Schwerpunkt beim Angebot von Fake Shops liegt nämlich in der Täuschung des Kunden. Für diese benötigt der Angreifer in erster Linie einen überzeugend wirkenden Onlineshop. Um einen solchen zu erstellen, nutzen die Angreifer häufig die folgenden Strategien.

1. Transportverschlüsselung

In den vergangenen Jahren wurde im Rahmen von Aufklärungskampagnen zur IT-Sicherheit häufig suggeriert, dass eine Webseite mit TLS- bzw. SSL-Verschlüsselung per se vertrauenswürdig sei. So sollten sich Nutzer etwa auf das „grüne Schloss" oder das „https" vor der eigentlichen Internetadresse verlassen.[6] Grundsätzlich bewirkt eine TLS- bzw. SSL-Verschlüsselung jedoch nur, dass die Verbindung zum Webserver verschlüsselt erfolgt. Ein Identitätsnachweis oder gar eine Bestätigung der Seriosität der Gegenseite lässt sich aus der Verschlüsselung grundsätzlich nicht herleiten. Angreifer sind daher vermehrt dazu übergegangen, ihre Webseiten ebenfalls verschlüsselt anzubieten und so das falsche Sicherheitsgefühl potentieller Opfer hinsichtlich der Vertrauenswürdigkeit auszunutzen.[7] Ein Beleg dafür ist, dass bereits im November 2018 fast die Hälfte aller Phishing-Webseiten auf diesen Trick zurückgriff.[8] Etwas anderes gilt lediglich bei sog. Extended-Validation-Zertifikaten, die einen Identitätsnachweis beinhalten. Da der Sicherheitsgewinn durch die Zertifikate nicht zuletzt wegen unzureichender Wahrnehmung durch den Nutzer jedoch gering ist, werden sie beispielsweise von den Browsern Chrome und Firefox nicht mehr unterstützt und werden daher zukünftig an Bedeutung verlieren.[9]

---

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 10. 3. 2021.

1 BKA, Bundeslagebild Cybercrime 2019 vom 30. 9. 2020, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

2 Bitkom, Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr.

3 Die PKS 2019 des BKA weist in der Grundtabelle „Tatmittel Internet" zwar verschiedene potenziell passende Kategorien aus (Warenbetrug, Betrug, Warenkreditbetrug), allerdings lässt sich nur erahnen, welchen Anteil Fake Shops an diesen Kategorien haben.

4 MMR-Aktuell 2019, 421351.

5 MMR-Aktuell 2020, 428160.

6 Vgl. z. B. *Kornherr*, HTTPS-Verschlüsselung: Ein grünes Schloss für Ihre Sicherheit, 30. 11. 2016, online abrufbar unter https://web.de/magazine/in-eigener-sache/https-gruenes-schloss-sicherheit-32038452.

7 *Scherschel*, Browser-Sicherheit: Grünes Schloss heißt noch lange nicht sicher, heise.de, 27. 11. 2018, online abrufbar unter https://www.heise.de/newsticker/meldung/Browser-Sicherheit-Gruenes-Schloss-heisst-noch-lange-nicht-sicher-4233702.html.

8 *Krebs*, Half of all Phishing Sites Now Have the Padlock, KrebsonSecurity, 26. 11. 2018, online abrufbar unter https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/.

9 *Böck*, Browser wollen teure Zertifikate nicht mehr hervorheben, Golem.de, 12. 8. 2019, online abrufbar unter https://www.golem.de/news/extended-validation-browser-wollen-teure-zertifikate-nicht-mehr-hervorheben-1908-143151.html.

2. Kopieren von Inhalten seriöser Onlineshops

Darüber hinaus orientieren sich die Angreifer auch an anderer Stelle an seriösen Onlineshops und übernehmen beispielsweise deren Produktbeschreibungen oder Werbefotos. In diesem Zusammenhang kopieren die Angreifer gerne auch Gütesiegel, beispielsweise das des gleichnamigen Unternehmens „Trusted Shops", um Vertrauenswürdigkeit zu suggerieren. Den Angreifern kommt dabei zugute, dass viele Nutzer die Echtheit der Siegel auf Webseiten nicht überprüfen, sondern bereits bei deren Anblick davon ausgehen, dass dieses ordnungsgemäß erteilt wurde. In diesem Zusammenhang nutzen die Täter mitunter auch professionelle Suchmaschinenoptimierung oder kaufen positive Bewertungen, um die Attraktivität des Fake Shops zu steigern.[10]

3. Täuschung durch Call-Center

Um den Shop möglichst lange am Leben zu halten und auch Nutzer erreichen zu können, die eher vorsichtig beim Online-Shopping sind, bieten die Angreifer mitunter sogar Service-Rufnummer an.[11] Hinter diesen stehen dann üblicherweise Call-Center, die entweder selbst betrogen werden oder Teil des kriminellen Netzwerkes sind. Sie sollen skeptische Interessenten im Rahmen des Gesprächs dann zum Kauf über den Fake Shop überreden oder bereits bestellte Kunden durch eine Verzögerungstaktik von einer Anzeige oder weiteren Schritten gegen den Fake Shop abhalten, damit dieser weiterhin von den Angreifern genutzt werden kann.

4. Automatisierte Erstellung neuer Shops

Fake Shops sind stets ein Geschäft auf Zeit. So führen nicht nur Beschwerden von geprellten Kunden, sondern auch die Urheberrechtsverletzungen durch das Kopieren von Inhalten anderer Shops regelmäßig dazu, dass die betreffenden „Angebote" vergleichsweise rasch verschwinden. Die Angreifer wirken dem durch die automatisierte und fortlaufende Stellung neuer Fake Shops entgegen. Die Bereitstellung von „schlüsselfertigen" Fake Shops erfolgt teilweise auch als kriminelle Dienstleistung im Rahmen von „Cybercrime as a Service".[12] Dabei können vorinstallierte Fake Shops über kriminelle Online-Marktplätze erworben und im Anschluss betrieben werden. Dieses arbeitsteilige Vorgehen der Täter erschwert nicht nur die Aufklärung der Straftaten, sondern macht es auch Angreifern mit geringem technischem Know-how möglich in den Betrieb von Fake Shops einzusteigen.

III. Polizeiliche Takedown-Requests und deren rechtliche Einordnung

Obwohl die Problematik von Fake Shops bereits hinlänglich bekannt ist, fehlt es scheinbar nach wie vor an wirksamen Methoden, die kriminellen Aktivtäten einzudämmen. Immer häufiger kommt es daher im Rahmen der insbesondere für das repressive Vorgehen bedeutsamen Bestandsdatenauskunftsersuchen nach § 113 TKG vor, dass die Behörden um Abschaltung der Website bitten. Gelegentlich wird dabei auch pauschal auf das landeseigene Polizeigesetz verwiesen oder es werden „Belege" mit dem Hinweis auf oben bereits erwähnte Warnlisten oder Online-Foren beigefügt. Dieses Vorgehen wird im Folgenden insgesamt mit dem Begriff „Takedown-Request" umschrieben. Der Gedanke hinter den polizeilichen Takedown-Requests ist, dass durch die Abschaltung des Fake Shops durch den Hosting-Anbieter weitere Bestellungen effektiv unterbunden werden können. Hierdurch reduziert sich der Zeitraum, in dem die Täter über den Fake Shop Geld erwirtschaften können, während gleichzeitig der Aufwand für die Erstellung neuer Fake Shops steigt. Eine sehr schnelle Sperrung von Fake Shops könnte damit letztlich dazu führen, dass das Geschäftsmodell für die Täter mit zu hohem Aufwand verbunden ist und sich daher finanziell nicht mehr lohnt. Andererseits sind polizeiliche Takedown-Requests nicht spezialgesetzlich regelt, weshalb sich die Frage stellt auf welcher Rechtsgrundlage die Polizei gegenüber dem Hosting-Anbieter tätig werden kann.

1. Kein Tätigwerden zur Strafverfolgung

Eine Legitimation des polizeilichen Handelns könnte sich aus der Ermittlungsgeneralklausel des § 163 Abs. 1 S. 1 StPO ergeben. Bestandsdatenauskunftsersuchen oder Überwachungsmaßnahmen an der technischen Infrastruktur dienen der Erforschung der Sach- und Gefahrenlage oder der Beweissicherung. Es handelt sich bei den regelmäßig im Zusammenhang mit Fake Shops verübten Taten auch um Straftaten, nämlich um Formen des Betrugs (§ 263 StGB). Die Täter nutzen die Website als Werkzeug zur Täuschung des Opfers, das daraufhin eine Vermögensverfügung zugunsten der Täter vornimmt. Der gelegentlich fälschlicherweise angenommene Computerbetrug (§ 263a StGB) ist hingegen im umgekehrten Fall einschlägig, wenn der Täter nicht der Händler, sondern der vermeintliche Kunde ist und die Website dazu nutzt eine Bestellung unter Verwendung fremder Zahlungsdaten abzusetzen.[13]

2. Präventiver Charakter der Maßnahme

Der Takedown-Request dient jedoch in erster Linie der Verhinderung weiterer Straftaten, da sie für sich genommen nicht geeignet ist, zur Aufklärung des Sachverhalts beizutragen. Demnach handelt es sich um eine rein präventive Maßnahme. Die Rechtsgrundlage ist daher im Gefahrenabwehrrecht zu suchen. Sonderzuweisungen sind im Bereich der früher noch als Teledienste bezeichneten Internetdienste nicht einschlägig. Gemäß § 4 BKAG ist das Bundeskriminalamt originär zuständig für die Strafverfolgung im Bereich der organisierten Kriminalität. Wie bereits dargestellt wurde, handelt es sich bei den Straftaten im Zusammenhang mit Fake Shops gerade nicht um Computerbetrugsstraftaten, sodass § 4 Abs. 1 Nr. 5 4. Alt. BKAG ausscheidet, der darüber hinaus auch an den weiteren Voraussetzungen scheitern würde. Demnach kann eine Zuständigkeit des BKA für die Strafverfolgung bestenfalls durch Ersuchen einer Landesbehörde begründet werden (§ 4 Abs. 3 Nr. 2 BKAG). Eine originäre Zuständigkeit des BKA zur Gefahrenabwehr ist nach § 5 BKAG nur bei der Abwehr von Gefahren des internationalen Terrorismus gegeben. Als Rechtsgrundlage für Takedown-Requests kommen daher lediglich die landeseigenen polizeilichen Generalklauseln in Betracht.[14]

10 *Behr*, Prozess in Frankfurt: Virtuelle Technik aus der Türkei kostete Millionen, Frankfurter Rundschau, 6. 3. 19, online abrufbar unter https://www.fr.de/frankfurt/virtuelle-technik-tuerkei-kostete-millionen-11829561.html.

11 *Haug-Peichl*, Nach Vorkasse verschwunden, mainpost.de, 15. 12. 2015, online abrufbar unter https://www.mainpost.de/ueberregional/wirtschaft/mainpostwirtschaft/Nach-Vorkasse-verschwunden;art9485,9048905.

12 T3N, Fake Shops: Wie ein Einzeltäter rund 440 000 Euro ergaunerte, t3n.de, 10. 5. 2017, abrufbar unter https://web.archive.org/web/20171121005759/http://t3n.de/news/fake-shops-einzeltaeter-rund-821734/.

13 *Ullenboom*, NZWiSt 2018, 26, 27; *Ceffinato*, JuS 2019, 337, 340.

14 *Zimmermann*, NJW 1999, 3145, 3146.

3. Sachliche und örtliche Zuständigkeit der Polizeibehörde

Die sachliche Zuständigkeit der Polizei- und Ordnungsbehörden der Länder folgt mangels spezialgesetzlicher Zuordnung aus dem allgemeinen Polizei- und Ordnungsrecht, beispielsweise aus §§ 10 ff. POG NRW. Im Gegensatz zur sachlichen Zuständigkeit, wirft jedoch vor allem die örtliche Zuständigkeit Fragen auf. Soweit von einem Internetdienst eine polizeiliche Gefahr ausgeht, bestimmt sich die örtliche Zuständigkeit nach den jeweiligen polizeirechtlichen Bestimmungen. Demnach ist jeweils die Ordnungsbehörde örtlich zuständig, in deren Bezirk entweder die zu schützenden Interessen verletzt oder gefährdet werden (vgl. § 7 Abs. 1 POG NRW) oder in deren Bezirk eine polizeiliche Aufgabe wahrzunehmen ist (vgl. § 81 Abs. 1 SPolG). Kennzeichnend für die Gefahren, die von Internetdiensten ausgehen ist jedoch gerade die überörtliche Verfügbarkeit der Dienste und damit auch die überörtliche Gefahr. Es erscheint daher zweckmäßig, polizeiliche Aufgaben in diesem Bereich nicht lediglich in benachbarten Bezirken einheitlich zu regeln, wie dies das Polizei- und Ordnungsrecht regelmäßig ermöglicht (vgl. § 4 Abs. 2 OBG NRW; § 81 Abs. 3 SPolG). Eine solche überörtliche Zuständigkeit von Polizei- und Ordnungsbehörden ist vorliegend jedoch nicht ersichtlich, sodass regelmäßig mehrere Behörden ihre örtliche Zuständigkeit aus der Tatsache herleiten, dass es Geschädigte in ihrem Polizeibezirk gibt.

4. Erforderlichkeit einer Rechtsgrundlage

Unabhängig von der Zuständigkeit der Polizeibehörden stellt sich die Frage, ob ein Takedown-Request durch die Polizei einer Rechtsgrundlage bedarf. Dies ist der Fall, wenn die mit dem Takedown-Request verbundene Bitte einen gewichtigen Eingriff in ein Grundrecht des Hosting-Anbieters darstellt.[15] Da es sich um eine bloße Bitte gegenüber dem Hosting-Anbieter handelt und keine Rechtsfolge angedroht wird, könnte man zunächst annehmen, ein Eingriff in ein Grundrecht, insbesondere die Berufsfreiheit des Hosting-Anbieters, nicht in Betracht kommt. Hierbei wird jedoch vernachlässigt, dass es sich bei der Polizei um einen staatlichen Akteur handelt und – ähnlich wie bei einer Gefährderansprache – in den Schutzbereich eines Grundrechts auch faktisch oder mittelbar eingegriffen werden kann.[16] Bei polizeilichen Takedown-Requests könnte dies insbesondere der Fall sein, wenn die Maßnahme über einen Einschüchterungs- und Abschreckungseffekt auf die Entschließungsfreiheit[17] des Hosting-Anbieters einwirkt. Ob dies in der Praxis der Fall ist, kann nur anhand einer Einzelfallanalyse entschieden werden, bei der insbesondere die Unternehmensgröße des Hosting-Anbieters, das Vorhandensein von juristischer Expertise sowie die im Anschreiben der Polizeibehörde gewählte Formulierung eine Rolle spielt. Vor diesem Hintergrund ist ein Einschüchterungs- und Abschreckungseffekt bei polizeilichen Takedown-Requests im Einzelfall nicht auszuschließen. In diesen Konstellationen wäre demnach eine Rechtsgrundlage erforderlich. Als solche kommt in Ermangelung einer spezialgesetzlichen Regelung in den Polizeigesetzen der Länder, deren Notwendigkeit mit Blick auf die Grundrechtsintensität der Maßnahme im Einzelfall zu diskutieren wäre,[18] nur die polizeiliche Generalklausel (vgl. § 8 Abs. 1 PolG NRW; § 8 Abs. 1 SPolG) als Rechtsgrundlage in Betracht. Eine öffentlich-rechtliche Störerhaftung des Hosting-Anbieters[19] sowie das Vorliegen einer Gefahr im Sinne des Polizeirechts dürften hingegen in der Regel keine besonderen rechtlichen Herausforderungen verursachen.

IV. Rechtsfolgen für Hosting-Anbieter

Da es sich bei den polizeilichen Takedown-Requests dem Wortlaut nach häufig um eine bloße Bitte handelt, lösen die Schreiben in der Regel keine unmittelbare Rechtsfolge aus. Hieraus folgt jedoch nicht, dass die polizeiliche Information über einen mutmaßlichen Fake Shop keinerlei rechtliche Auswirkung hätte. Zu denken ist hier insbesondere an die Zerstörung der Haftungsprivilegierung des Hosting-Anbieters nach § 10 TMG und Schadensersatzansprüche von Kunden in Fällen in denen tatsächlich kein Fake Shop vorliegt.

1. Die Haftungsprivilegierung des Hosting-Anbieters

Die Haftungsprivilegierung des § 10 TMG schützt den Hosting-Anbieter, als Diensteanbieter im Sinne von § 2 Nr. 1 TMG, vor einer Haftung für die Speicherung von fremden Informationen seiner Nutzer.[20] Im Kontext von Fake Shops wäre eine solche beispielsweise wegen Beihilfe der über den Fake Shop begangenen Betrugsstraftaten bzw. deren Versuch denkbar.[21] In Betracht kommen auch Verletzungen von Namens-, Marken- oder Urheberrechten Dritter, da die Betreiber von Fake Shops beim Versuch, ihr Angebot möglichst realistisch wirken zu lassen, häufig rechtlich geschützte Inhalte Dritter verwenden.

Die Haftungsprivilegierung greift nach vgl. § 10 S. 1 Nr. 1 Hs. 1 TMG jedoch nur, wenn der Diensteanbieter keine Kenntnis von der Rechtswidrigkeit der Handlung bzw. Information hat.[22] Erlangt der Diensteanbieter Kenntnis von der Rechtswidrigkeit, muss er, um weiterhin von der Haftungsprivilegierung zu profitieren nach § 10 S. 1 Nr. 2 TMG, unverzüglich tätig werden und die rechtswidrigen Inhalte löschen oder den Zugang zu ihnen sperren.[23] Hierbei kommt es auf den Weg der Kenntniserlangung nicht an.[24] Zu einer aktiven Überprüfung von Inhalten im Sinne einer Beobachtungspflicht ist der Hosting-Anbieter jedoch nicht verpflichtet.[25] Die Kenntnis von der Rechtswidrigkeit der Nutzerinhalte ist folglich für die Haftungsprivilegierung des § 10 TKG von zentraler Bedeutung. Kenntnis im Sinne des § 10 S. 1 Nr. 1 TMG bedeutet dabei positive Kenntnis von der Rechtswidrigkeit der Inhalte. Ein bloßes Kennenmüssen oder eine fahrlässige Unkenntnis sind hingegen nicht ausreichend.[26] Zur Kenntniserlangung ist darüber hinaus erforderlich, dass der Hosting-Anbieter eine konkrete Kenntnis vom Inhalt der rechtswidrigen Informa-

15 VG München, 18. 2. 2020 – M 7 K 18.5065, BeckRS 2020, 5093.
16 VG München, 18. 2. 2020 – M 7 K 18.5065, BeckRS 2020, 5093.
17 VGH Mannheim, 7. 12. 2017 – 1 S 2526/16, BeckRS 2017, 137291; *Hebeler*, NVwZ 2011, 1361, 1365; *Kießling*, DVBl 2012, 1210.
18 BVerwG, 25. 7. 2007 – 6 C 39/06, NVwZ 2007, 1439, 1441.
19 *Spindler*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2018, § 10 TMG, Rn. 118.
20 *Müller-Broich*, Telemediengesetz, 2012, § 10 TMG, Rn. 1; *Altenhain*, in: MüKo StGB, 3. Aufl. 2019, § 10 TMG, Rn. 6.
21 Vgl. zur Strafbarkeit: LG München I, 7. 6. 2017 – 19 KLs 30 Js 18/15, BeckRS 2017, 127611.
22 *Hoffmann/Volkmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 10 TMG, Rn. 22.
23 *Altenhain*, in: MüKo StGB (Fn. 20) § 10 TMG, Rn. 23 f.
24 *Paal*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 28 Ed., Stand: 1. 2. 2020, § 10 TMG, Rn. 23; *Sobola/Kohl*, CR 2005, 443, 447; *Spindler*, NJW 2002, 921, 924.
25 *Spindler*, in: Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 10 TMG, Rn. 20.
26 *Paal*, in: Gersdorf/Paal (Fn. 24), § 10 TMG, Rn. 24.

tion oder Handlung erhält.[27] Eine allgemeine Mitteilung an den Anbieter ist nicht ausreichend.[28]

Im Rahmen ihrer Takedown-Requests bezeichnen die Polizeibehörden in der Regel sehr genau, bei welcher Webseite sie von einem Fake Shop ausgehen. In diesen Fällen wird man von einer konkreten Kenntnis des Inhalts ausgehen können. Teilweise enthalten die Takedown-Requests jedoch nur die Angabe einer IP-Adresse ohne weitergehende Informationen. Dies ist gerade in Fällen des sog. Shared-Hosting, bei dem ein Server mit einer IP-Adresse eine Vielzahl von Webseiten ausliefert, tendenziell nicht geeignet, um eine konkrete Kenntnis auszulösen. Über die konkrete Kenntnis der betroffenen Informationen hinaus, setzt eine Kenntniserlangung im Sinne des § 10 S. 1 Nr. 2 TMG auch eine Kenntnis von der Rechtswidrigkeit der Information oder Handlung voraus.[29] Kenntnis liegt vor, wenn die Rechtsverletzung für den Diensteanbieter offenkundig ist oder ihm dargelegt wird.[30] Ergibt sich der Rechtsverstoß, wie z. B. bei einer offensichtlichen Beleidigung, nicht eindeutig bereits aus der beanstandeten Information, ist zur Kenntniserlangung eine Darlegung der Rechtswidrigkeit erforderlich.[31] Dem Hinweisgeber obliegt insoweit die Mitteilung der den Rechtsverstoß begründenden Tatsachen und Wertungen.[32] Belege müssen nicht beigefügt werden, können aber vom Diensteanbieter bei berechtigten Zweifeln verlangt werden.[33] Vor diesem Hintergrund ist eine Einzelfallbeurteilung geboten, bei der zwischen dem Betrieb des Fake Shops als strafbare Handlung, und der denkbaren Verwendung von rechtswidrigen Informationen, wie z. B. marken- oder urheberrechtlich geschützten Inhalten, zu trennen ist. Die Folgen eines Takedown-Requests auf die Haftungsprivilegierung des § 10 TKG lassen sich damit nicht einheitlich beurteilen.

2. Ertragsrechtliche Konsequenzen

Ebenso uneinheitlich sind die Auswirkungen von polizeilichen Takedown-Request auf die Vertragsbeziehung zwischen Hosting-Anbieter und dem jeweils betroffenen Kunden. Klar dürfte insoweit zunächst sein, dass der Hosting-Anbieter nicht dazu verpflichtet ist, rechtswidrige Handlungen seines Kunden bzw. die Speicherung rechtswidriger Informationen zu dulden. Viele Hostingverträge erhalten hierzu auch eindeutige Klauseln.[34] Weniger einfach zu beurteilen ist die Rechtslage, wenn die Polizei in ihrem Takedown-Request fälschlicherweise davon ausgeht, dass ein Fake Shop vorliegt und der Hosting-Anbieter den Onlineshop sodann sperrt. In diesem Szenario könnte der Hosting-Kunde auf die Idee kommen, Schadensersatzansprüche, etwa wegen durch die Sperrung entgangenen Einnahmen, gegenüber dem Hosting-Anbieter geltend zu machen. Ob ein solcher Versuch von Erfolg gekrönt ist, hängt zunächst von etwaigen Vereinbarungen im Hostingvertrag ab. Denkbar wären insoweit einerseits Klauseln, die den Hosting-Anbieter bei polizeilichen Anfragen pauschal zur Sperrung berechtigten. Existieren solche Klauseln nicht, wird der Hosting-Anbieter einen polizeilichen Takedown-Request jedoch zumindest einer Plausibilitätsprüfung unterziehen müssen. Eine solche kann beispielsweise durch eine genauere Prüfung der im Kundenkonto hinterlegten Daten, Rückfragen beim Kunden oder teilweise bzw. temporäre Einschränkungen des Hosting Services erfolgen. Zum Nachweis in Konfliktsituationen sollte der Prozess genau definiert und dokumentiert werden. Je weniger Informationen der Hosting-Anbieter im Rahmen des Takedown-Requests zur Verfügung gestellt bekommt, desto schwieriger wird die Rechtfertigung vertraglicher Konsequenzen.

3. Konsequenzen beim „Weitersagen“

Gem. § 113 Abs. 4 S. 2 TKG darf der Hosting-Anbieter seinen Kunden nicht über ein Bestandsdatenauskunftsersuchen informieren.[35] Darauf weisen Behörden in ihren standardisierten Schreiben regelmäßig hin. Gehen zur selben Domain allerdings mehrere Ersuchen ein und wird in einigen um die Abschaltung gebeten, so stellt sich die Frage, ob der Anbieter gegen das Verbot zur Information des Kunden verstößt, sobald er die Website abschaltet. Immerhin ist anzunehmen, dass der Betreiber eines Fake Shops vom Abschalten seiner Website darauf schließen kann, dass Ermittlungen eingeleitet wurden.

Die Abschaltung eines Fake Shops kann außerdem in Konflikt geraten mit einem Beschluss zur Serverüberwachung, der nach § 100a Abs. 1 und 2 Nr. 1 lit. n i. V. m. § 263 Abs. 3 S. 2 StGB in einigen Konstellationen möglich ist. Ein Verstoß gegen die Verschwiegenheitspflicht ist nach § 149 Abs. 1 Nr. 35, Abs. 2 TKG bußgeldbewehrt.

Es ist fraglich, ob das Abschalten des Fake Shops bereits als Verletzung der Verschwiegenheitsverpflichtung zu interpretieren ist. Dagegen spricht, dass § 113 Abs. 4 S. 2 TKG ausdrücklich auf das zu wahrende Stillschweigen abstellt. Es lässt sich argumentieren, dass das Stillschweigen gegenüber dem Betroffenen durch die Abschaltung nicht gebrochen wird. Zwar könnte auch eine nicht an den Betroffenen adressierte Handlung geeignet sein, das Stillschweigen zu brechen, wenn aus ihr eindeutig hervorgeht, dass ein Auskunftsersuchen eingegangen ist. Allerdings ist für den Betroffenen nicht ohne weiteres ersichtlich, ob die Abschaltung aufgrund eines polizeilichen Ersuchens erfolgte oder ob der Provider aufgrund einer Abuse-Meldung einen Verstoß gegen die AGB festgestellt hat und diesen der Abschaltung zugrunde legt. Dafür spricht allerdings der Sinn und Zweck der Verschwiegenheitsverpflichtung, der darin besteht den Erfolg laufender Ermittlungen nicht zu gefährden und deren Offenlegung zu verhindern.[36] Zunächst kann die Abschaltung einer Website ähnlich einem Warrant Canary[37] ein deutlicher Hinweis für den Betroffenen sein, dass behördliche Maßnahmen eingeleitet wurden. Das ist insbesondere dann anzunehmen, wenn zuvor keine Information über etwaige Abuse-Meldungen an den Betroffenen erfolgt. Demnach bestünde aus Sicht des Betroffenen ein erkennbarer Unterschied zur sofortigen und dauerhaften Abschaltung aufgrund eines behördlichen Ersuchens. Darüber hinaus kann die Abschaltung im Widerspruch zu einer Maßnahme nach § 100a StPO (Server-TKÜ) stehen, sodass laufende Ermittlungen gefährdet würden, einerseits, weil ein abgeschalteter Server nicht

27 *Spindler*, in: Spindler/Schmitz (Fn. 25), § 10 TMG, Rn. 24.
28 *Spindler*, in: Spindler/Schmitz (Fn. 25), § 10 TMG, Rn. 24.
29 *Spindler*, in: Spindler/Schmitz (Fn. 25), § 10 TMG, Rn. 28 f.
30 *Altenhain*, in: Müko StGB (Fn. 20), § 10 TMG, Rn. 14.
31 *Altenhain*, in: Müko StGB (Fn. 20), § 10 TMG, Rn. 14.
32 BGH, 17. 8. 2011 – I ZR 57/09, GRUR 2011, 1038.
33 *Altenhain*, in: Müko StGB (Fn. 20), § 10 TMG, Rn. 14.
34 Vgl. etwa: *Stummel*, in: Vertragsformulare PREMIUM, 13.5.1.1 Web Hostingvertrag, § 3 Abs. 3.
35 *Graulich*, in: Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 113 TKG Manuelles Auskunftsverfahren, Rn. 48.
36 Entwurfsbegründung zu § 87 TKG-E, BT-Drs. 13/3609, S. 56.
37 Ein Warrant Canary ist eine Methode, mit der ein Anbieter seine Nutzer darüber informiert, dass dem Anbieter eine staatliche Anordnung zugestellt wurde, obwohl es gesetzlich verboten ist, die Existenz der Vorladung offenzulegen. Dazu informiert der Warrant Canary den Benutzer in der Regel darüber, dass zu einem bestimmten Datum keine gerichtliche Anordnung vorliegt.

mehr überwacht werden kann, andererseits weil die Abschaltung eines Fake Shops für den Betroffenen auch eben dargestellte Warnfunktion haben kann, sodass auch Ermittlungen in Bezug auf weitere vom selben Betroffenen betriebene Fake Shops gefährdet würden. Durch Takedown-Requests und insbesondere durch sich widersprechende Anordnungen und Bitten schaffen Behörden daher ein ungeklärtes Haftungsrisiko für den Hosting-Anbieter.

V. Fazit

Über Fake Shops können Kriminelle mit Hilfe geschickter Täuschung auch ohne größeres technisches Wissen erfolgreich Kasse machen. Gleichzeitig scheinen bisher effiziente Mittel zur erfolgreichen Bekämpfung von Fake Shops zu fehlen. Ob polizeiliche Takedown-Requests – als bloße Bitte zur Löschung oder Sperrung eines Fake Shops – als neue Wunderwaffe angesehen werden können, ist insbesondere mit Blick auf die Unverbindlichkeit der Maßnahme fraglich. Vor dem Hintergrund, dass es bisher einerseits an einer klaren Regelung für das polizeiliche Vorgehen fehlt und andererseits negative rechtliche Konsequenzen für Hosting-Anbieter drohen, ist der Gesetzgeber jedoch dazu aufgerufen die genutzten Maßnahmen zu evaluieren und bei Bedarf eine klare rechtliche Regelung zu schaffen.

Regierungsrat Dr. Simon Schwichtenberg*

Fehlende Umsetzung der DSRL-JI: Warum der Gesetzgeber bislang kein guter Türsteher ist

Unzureichende Rechtsgrundlagen bei Datenübermittlung an und Datenzugriff durch Ermittlungsbehörden

Kurz und Knapp

Datenübermittlungen an Ermittlungsbehörden und der Zugriff durch Behörden sind in den Fokus der Aufmerksamkeit gerückt. Der folgende Beitrag soll zeigen, dass der Thematik unabhängig von „Corona-Gästelisten" und Anlässen und Formen der Datenspeicherung eine Kernproblematik zugrunde liegt: Es fehlen geeignete Rechtsgrundlagen, nicht zuletzt vor dem Hintergrund von mehr als 1000 Tagen fehlender Umsetzung der DSRL-JI. Der Gesetzgeber sollte nun bei dieser alle betreffenden Thematik für Sicherheit sorgen.

I. Unsicherheiten bei der Datenübermittlung und beim Datenzugriff

Ermittlungsbehörden, allen voran die Staatsanwaltschaft und die Polizei, sind im Rahmen ihrer Ermittlungstätigkeiten auf Informationen und auf Quellen, die ihnen diese Informationen zur Verfügung stellen, angewiesen. Sie wollen und müssen vorhandene Informationsquellen nutzen. Wie eine Art Naturgesetzmäßigkeit erschien aus diesem Grunde das aktuellste Beispiel, dass Polizeibehörden Zugriff auf sog. „Corona-Gästelisten" nehmen wollten und genommen haben, um etwa herauszufinden, wer sich wann wo aufgehalten hat. Die Zulässigkeit dieser Form der Informationsbeschaffung wird durchaus unterschiedlich beurteilt.[1]

Die geführten Diskussionen zeigen aber vor allem eines: es fehlen – unabhängig von „Corona-Gästelisten", den Anlässen, den speichernden Stellen und den Formen der Datenspeicherung (analog oder digital) – geeignete Rechtsgrundlagen sowohl für die Datenübermittlung an Ermittlungsbehörden als auch für den Datenzugriff durch Behörden.

Nach dem sog. „Doppeltürmodell" des BVerfG benötigen übermittelnde (private) Stellen für die Datenübermittlung und Ermittlungsbehörden für den Datenzugriff jeweils eine Legitimationsgrundlage. Vorhandene Erlaubnistatbestände für eine Datenübermittlung können bei übermittelnden Stellen jedoch nicht für Rechtssicherheit sorgen, da mit ihnen z. T. unerfüllbare Prüfpflichten einhergehen. Solche legt vor allem § 24 Abs. 1 Nr. 1 BDSG auf, aber – auf Länderebene – etwa auch § 57 BremPolG. Doch selbst wenn eine Datenübermittlung an Behörden gerechtfertigt ist, fehlt es häufig an europarechtskonformen Rechtsgrundlagen für den Datenzugriff. Dieses Fehlen ist durch die bisher mangelhafte Umsetzung der „kleinen Schwester der DSGVO",[2] der DSRL-JI, bedingt.

Der nationale Gesetzgeber ist somit gefordert, im Sinne des „Doppeltürmodells" des BVerfG sowohl geeignete Rechtsgrundlagen für die Datenübermittlung als auch für den Zugriff zu schaffen. Übermittelnden Stellen sollte er nur solche Prüfpflichten auferlegen, die sie tatsächlich erfüllen können. Die Hauptlast der Prüfpflichten sollte er bei Ermittlungsbehörden verorten – anderweitig bleibt er ein ziemlich schlechter Türsteher.

II. Zwei Rechtsgrundlagen und zwei Verantwortliche: das „Doppeltürmodell" des BVerfG

Das sog. „Doppeltürmodell" des BVerfG verlangt, dass sowohl die Datenübermittlung an Behörden als auch der

* Mehr über den Autor erfahren Sie auf S. VIII. Der Beitrag gibt ausschließlich die persönlichen Ansichten des Autors wieder. Alle zitierten Internetquellen wurden zuletzt abgerufen am 9. 3. 2021.

1 S. bspw. *Niedernhuber*, KriPoZ 2020, 318 ff.; *Bloß/Kühorn*, JURA 2020, 1036 ff.; Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Zweckbindung von personenbezogenen Daten zur Verfolgung von Infektionsketten (Pressemitteilung v. 23. 7. 2020); ZD-Aktuell 2020, 07242.

2 S. hierzu bereits *Schwichtenberg*, DuD 2016, 605.