05.03.2019

Projektgruppe „Bekämpfung von Fakeshops“ der
Arbeitsgruppe Wirtschaftlicher Verbraucherschutz

„Bekämpfung von Fakeshops“

Bericht der Projektgruppe der AG WV
zum Arbeitsauftrag aus TOP 37 der 14. VSMK in Saarbrücken

[redacted]

Inhaltsverzeichnis

A. Einführung

I. Ausgangslage

Die 14. Verbraucherschutzministerkonferenz hat sich im Juni 2018 unter TOP 37 mit der „Bekämpfung von Fake-Shops“ im Internet beschäftigt und die Arbeitsgruppe Wirtschaftlicher Verbraucherschutz (AG WV) gebeten, gemeinsam mit den Verbraucherverbänden, dem Bundesministerium der Justiz und für Verbraucherschutz (BMJV) sowie mit den Ermittlungsbehörden der Länder geeignete Maßnahmen zur Bekämpfung von Fake-Shops zu prüfen. In die Prüfung sollten auch die nationalen Umsetzungsmaßnahmen der novellierten Verordnung (EU) Nr. 2017/2394 über die Zusammenarbeit der nationalen zuständigen Behörden im wirtschaftlichen Verbraucherschutz (CPC-Verordnung), die Einrichtung und Ausgestaltung einer bundeseinheitlichen Meldestelle für Fake-Shops sowie die Regelungen bei der Vergabe einer Domain einbezogen werden.

An der Arbeit der von der AG WV eingesetzten Projektgruppe beteiligten sich die Länder Baden-Württemberg (PG-Vorsitz), Bayern, Brandenburg, Niedersachsen und Nordrhein-Westfalen sowie das BMJV. Die Projektgruppe führte im November 2018 ein Gespräch mit Expertinnen und Experten aus den Verbraucherverbänden, der Wirtschaft, den Ermittlungsbehörden und der Domainregistrierungsstellen. Die Ergebnisse dieses Expertengespräches sind in die Meinungsbildung der Projektgruppe und den vorliegenden Bericht eingegangen.

Die Projektgruppe informierte sich außerdem über die Arbeit und Erfolge des österreichischen Projekts www.watchlist-internet.at.

II. Betroffenheit der Verbraucherinnen und Verbraucher

Der Marktwächter Digitale Welt hat im August 2018 eine Untersuchung zum Thema „Fake-Shops – Relevantes Verbraucherproblem in Deutschland“ veröffentlicht.[1] Unter „Fake-Shops“ wurden dabei solche Onlineshops verstanden, die rein aus betrügerischen Absichten geschaffen wurden und die betrieben werden, um Straftaten zu begehen. Alle Online-

[1] https://www.marktwaechter.de/sites/default/files/marktwaechter-untersuchung-fake-shops.pdf

Shops mit Lieferschwierigkeiten oder erheblichen Qualitätsmängeln zählten z.B. nicht dazu.

Die Projektgruppe hat sich dieser Definition von Fake-Shops angeschlossen und sich dementsprechend auf die Sachverhalte konzentriert, die in der Regel strafrechtlich als „Gewerbsmäßiger Betrug“ einzuordnen sind. Mit dem Verhalten von Onlineshops, bei denen es z.B. zu Beschwerden über Lieferprobleme, Servicemängel, lange Lieferzeiten oder andere Qualitätsmängel ging, hat sich die Projektgruppe nicht befasst, da in diesen Fällen andere Maßnahmen zu prüfen und zu diskutieren wären.

Anlass der Untersuchung des Marktwächters Digitale Welt waren konstante Beschwerden der Verbraucherinnen und Verbraucher bei den Verbraucherzentralen der Länder. Über sie erhält das Marktwächterteam bei der Verbraucherzentrale Brandenburg im Rahmen des Frühwarnnetzwerkes monatlich 10 - 20 neue Meldungen von Verbraucherinnen und Verbrauchern.

Die Untersuchung des Marktwächters Digitale Welt hatte das Ziel, das Ausmaß des Problems mit Fake-Shops zu ermitteln und Feststellungen über die Betroffenheit der Internet-Käufer in Deutschland zu treffen.

Die Untersuchung kommt im Rahmen einer repräsentativen Umfrage unter den Internet-Nutzern in Deutschland zu dem Ergebnis, dass jeder vierte deutsche Internetkäufer mindestens schon einmal Ware bestellt und die bezahlte Ware nicht erhalten haben dürfte. Aufgrund dieser Anzahl und in Verbindung mit weiteren Kriterien für das Vorhandensein eines Fake-Shops schätzt der Marktwächter Digitale Welt, dass in Deutschland über vier Millionen Verbraucherinnen und Verbraucher bereits einmal einem Fake-Shop zum Opfer gefallen sind.

Über eine automatisierte Google Abfrage konnten vom Marktwächter Digitale Welt etwa eine Million URLs (Uniform Resource Locator) ermittelt werden, die zu einem Fake-Shop führen. Über 90% dieser URLs verfügt über eine „.de-Adresse“. Solche Adressen genießen bei deutschen Verbraucherinnen und Verbrauchern ein besonderes Vertrauen. Auffällig war auch, dass der oder die Fake-Shop-Betreiber vorwiegend Domains verwendeten, die vom ursprünglichen Inhaber abgemeldet worden waren und die, nachdem die Domain-

Namen wieder zur Verfügung standen, von Fake-Shops übernommen wurden. Betroffen waren davon sowohl Privatpersonen als auch vielfach die ehemaligen Domain-Adressen von Anwälten, Ärzten, Politikern oder Verbänden und Parteien.

Die Projektgruppe hat zur Bekämpfung von Fake-Shops zwei wesentliche Felder behandelt: Zum einen wurde diskutiert, wie die Prävention und Information der Verbraucherinnen und Verbraucher verbessert werden kann, denn eine aufgeklärte und kritische Herangehensweise ist eine Möglichkeit, sich vor betrügerischen Aktivitäten zu schützen. Zum anderen wurde diskutiert, welche repressiven Maßnahmen – also z.B. Maßnahmen auf Seiten der Ermittlungsbehörden - einen Beitrag zur Bekämpfung von Fake-Shops leisten können.

Zivilrechtliche Instrumente, die z.B. den Verbraucherverbänden bei wettbewerbswidrigem Verhalten zur Verfügung stehen, hat die Projektgruppe nicht behandelt, da diese bei Fake-Shops in der Regel nicht greifen. Bei strafrechtlich relevanten Verhaltensweisen ist die Abmahnung oder Unterlassungserklärung kein primäres Mittel, um den gewerbsmäßigen Betrug zu unterbinden.

Die Projektgruppe hat sich nicht explizit mit Fake-Shops auf Online-Marktplätzen befasst. Hierzu hat bereits der Bundesrat im Juli 2018 (Beschluss Drs. 153/18) die EU Kommission um Prüfung gebeten, ob die Betreiber von Online-Marktplätzen verpflichtet werden könnten, im Rahmen des technisch und wirtschaftlich Möglichen die notwendigen Vorkehrungen zu treffen, um die Verbraucherinnen und Verbraucher besser vor unseriösen Anbietern, insbesondere vor sogenannten Fake-Shops, zu schützen.

B. Hauptteil

I. Derzeitige Maßnahmen der einzelnen Akteure zur Bekämpfung von Fake Shops und deren Grenzen

1. Präventive Maßnahmen

Eine Möglichkeit, die betrügerischen Aktivitäten von Fake-Shops zu erschweren, ist die Präventionsarbeit mit gezielten Presse-, Informations- und Beratungsmaßnahmen, um Verbraucherinnen und Verbraucher dafür zu sensibilisieren, die Anbieter im Online-Handel und deren Auftritte und Angebote kritisch zu betrachten. Sie sollen befähigt bzw. unterstützt werden, um anhand von kritischen Prüfungen Fake-Shops zu erkennen. Möglich ist z.B., die Orts- und Adressangabe im Impressum auf Plausibilität und Richtigkeit zu prüfen. Auch Ungereimtheiten und Auffälligkeiten bei einer Internetadresse können auf einen Fake-Shop hinweisen. Verbraucherinnen und Verbraucher sollten auch bei auffallend günstigen Preisen oder Kaufangeboten, die angeblich nur gegen Vorkasse „erworben“ werden können, aufmerksam werden und im Internet nach Erfahrungen anderer Verbraucherinnen und Verbraucher mit diesem Shop suchen.

Insbesondere Verbraucherorganisationen, die Polizei sowie die Verbraucherministerien der Länder bieten Maßnahmen zur Verbraucherinformation und zur Prävention an. Dazu gehören vor allem Informationen im Internet, schriftliche Hinweise und Broschüren, Vorträge, Veranstaltungen und Maßnahmen der Kriminalprävention. Beispielsweise wird in Veranstaltungen und Fortbildungen für die sensible Zielgruppe der Seniorinnen und Senioren auf Fake-Shops hingewiesen.

Die Verbraucherzentralen der Länder arbeiten bei der Präventionsarbeit zu Fake-Shops häufig mit der Polizei zusammen. Teilweise bestehen Kooperationsvereinbarungen zwischen Verbraucherzentralen und Landeskriminalämtern, die z.B. die Grundlage für gemeinsame Aktivitäten und/oder abgestimmte Informationsmaterialien darstellen.

Aber auch andere Akteure weisen auf die Problematik der Fake-Shops hin. Hinweise und Informationen für Verbraucherinnen und Verbraucher finden sich z.B. auf der Homepage des **De**utschen **N**etwork **I**nformation **C**enters (DENIC) oder des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom). Demgegenüber weisen seriöse Onlineshops in der Regel nicht auf die Risiken der Fake-Shops hin. Eine be-

sondere Bedeutung bei der Informations- und Präventionsarbeit haben die Medien. Sowohl in den Printmedien als auch in Rundfunk, Fernsehen und Internetmedien wird immer wieder auf betrügerische Aktivitäten von Fake-Shops hingewiesen.

Die Anzahl der Verbraucherbeschwerden und die Untersuchung des Marktwächters Digitale Welt deuten aber darauf hin, dass die Präventionsarbeit – zumindest im bisherigen Maß – alleine nicht ausreicht, das Problem des Betrugs durch Fake-Shops zu lösen. Dafür gibt es verschiedene Ursachen:

Zum einen fehlt es bei den Verbraucherinnen und Verbrauchern, die bisher noch nicht Opfer von Internetkriminalität waren, oft an der notwendigen Sensibilität. Macht ein Online-Shop optisch einen seriösen Eindruck, sind Verbraucherinnen und Verbraucher eher geneigt, einem solchen Shop zu vertrauen. Darüber hinaus werden manche Verbraucherinnen und Verbraucher bei den extrem günstigen Preisangaben, mit denen Fake-Shops ihre „Kunden“ locken, unvorsichtig. Zum anderen wird es für Verbraucherinnen und Verbraucher aber auch immer schwieriger, mit einfachen eigenen Prüfungen Fake-Shops zu erkennen. Die Gestaltung von Fake-Shops wird immer professioneller und es werden häufig real existierende Daten und Adressen verwandt.

Hinzu kommt, dass – auch nach den Beobachtungen der Verbraucherzentralen – Fake-Shops in der Regel nur sehr kurz im Netz auffindbar sind. Eine Ermittlungsbehörde hatte gegenüber der Projektgruppe z.B. darauf hingewiesen, dass manche Fake-Shops nur drei Tage online gestellt und beworben würden. Danach würden die Seiten wieder vom Netz genommen. Das macht das rechtzeitige Auffinden negativer Kundenaussagen im Netz fast unmöglich.

Präventionsmaßnahmen, die darauf abzielen, Verbraucherinnen und Verbraucher durch Informations- und Aufklärungsmaßnahmen zu befähigen, vor Abschluss einer Bestellung im Internet selbst tätig zu werden und den Anbieter und das Angebot kritisch auf Seriosität und Plausibilität zu überprüfen, werden deshalb auch in Zukunft allein nicht ausreichen, um Schäden durch Fake-Shops zu verhindern.

Die Verbraucherinformation und Präventionsarbeit will auch dafür sensibilisieren, dass Verbraucherinnen und Verbraucher, die bereits auf einen Fake-Shop hereingefallen sind,

aktiv werden. Betroffenen Verbraucherinnen und Verbrauchern wird in diesen Fällen geraten, sich an die Polizei oder die Verbraucherzentralen zu wenden. Da Fake-Shops aber immer professioneller betrieben und gestaltet werden, ist selbst für mit dem Phänomen vertrauten Stellen nicht ohne weiteres erkennbar, ob es sich um einen Fake-Shop handelt oder nur einen mangelhaft betriebenen Online-Shop.

2. Repressive Maßnahmen

a. Marktwächter: Eingang der einzelnen Meldungen der VZen

aa. Beschreibung

Der Marktwächter digitale Welt ist ein Frühwarnsystem, mit dem der Verbraucherzentrale Bundesverband und die Verbraucherzentralen den digitalen Markt aus der Perspektive der Verbraucherinnen und Verbraucher beobachten und analysieren. Grundlage dafür sind die Verbraucherbeschwerden, die bei den Verbraucherzentralen eingehen und empirische Untersuchungen. Auf dieser Basis sollen Fehlentwicklungen auf den Märkten und fragwürdige oder gesetzwidrige Geschäftsmodelle und Praktiken identifiziert werden. In konkreten Fällen werden Warnhinweise ausgesprochen, es können Informationen an zuständige Behörden weitergegeben werden oder Abmahnungen erfolgen.

Die Erkenntnisse des Marktwächters Digitale Welt basieren auf 10 – 20 monatlichen Beschwerden über Fake-Shops, die über die Verbraucherzentralen eingehen, und auf der unter A. bereits erwähnten Untersuchung vom August 2018. Diese Erkenntnisse werden vor allem für die Medien- und Öffentlichkeitsarbeit genutzt.

bb. Probleme/ Grenzen

In der Beratungsarbeit der Verbraucherzentralen werden betroffene Verbraucherinnen und Verbraucher dazu angehalten, Strafanzeige zu stellen, um so ggfs. ein Ermittlungsverfahren in Gang zu setzen. Nach der praktischen Erfahrung ist es allerdings wenig wahrscheinlich, dass die Betroffenen tatsächlich Anzeige erstatten, denn die Hoffnung, das gezahlte Geld dadurch zurück zu bekommen, ist gering. Dies führt allerdings dazu, dass die Strafverfolgungsbehörden nur ein sehr unvollständiges Bild über die Anzahl der Betroffenen, über die Täter und über die Methoden erhalten.

Eine systematische Übermittlung der Erkenntnisse des Marktwächters Digitale Welt an die Ermittlungsbehörden findet nicht statt. Die Informationen des Marktwächters Digitale Welt können eine konkrete Strafanzeige eines Betroffenen nicht ersetzen, sie wären aber als „Hintergrundinformation“ nutzbar. Ohne die Anzeigen der Betroffenen ist ein Betrug nicht nachweisbar. Selbst der Nachweis für einen versuchten Betrug würde voraussetzen, dass der Shop niemals vorhatte, die angebotene Ware zu liefern. Eine Übersendung als Hintergrundinformation für unter Umständen laufende Ermittlungsverfahren findet aber bestenfalls in Ausnahmefällen statt, da dem Marktwächter Digitale Welt in der Regel nicht bekannt ist, ob gegen einen Fake-Shop ermittelt wird und welche Staatsanwaltschaft diese Ermittlungen führt. Eine zentrale Anlaufstelle oder Erfassungsstelle, an die der Marktwächter Digitale Welt die Hinweise und Beschwerden der Verbraucherinnen und Verbraucher – ggf. auch aufbereitet und zusammengefasst – weitergeben könnte, ist nicht bekannt.

b. Ermittlungsmaßnahmen der Strafverfolgungsbehörden

aa. Beschreibung

Das Standardermittlungsverfahren stellt sich folgendermaßen dar: Ein erster Schritt bei Verdacht auf einen Fake-Shop ist eine Anfrage bei dem Domaininhaber / der Registrierungsstelle (wie z.B. DENIC), um Informationen zu dem technischen Hoster und den Anmeldedaten des Registrars zu erlangen (letztere sind zumeist Aliasteile). Über den Hoster kann der Serverstandort des Dienstes in Erfahrung gebracht werden, um eventuelle technische Maßnahmen (Serverüberwachung §§ 100a, 100g StPO) umzusetzen.

Des Weiteren kann eine Datenerhebung bei den Geschädigten und z.B. sog. Finanzagenten (Personen, die ihre Identität zur Kontoeröffnung zur Verfügung stellen) zur Konkretisierung der Einzeltaten und der näheren Umstände der Transaktionen erfolgen; Ziel ist dabei eine möglichst umfassende Sicherung von Kommunikationsspuren, auch in sozialen Netzwerken etc. (die Vorgehensweise der Täter ist häufig arbeitsteilig).

Ein weiterer Ansatzpunkt ist die Aufklärung sämtlicher Zielkonten, um den Zahlungsfluss nachzuverfolgen. So wird versucht, den Punkt zu finden, an dem die Gelder an die eigentlichen Täter ausgekehrt werden und den Finanzagentenkreislauf verlassen.

Es existiert das staatsanwaltschaftliche Zentralregister (ZStV), welches ein allgemeines Register ist, in dem zu Ermittlungsverfahren bei den Staatsanwaltschaften u.a. die Personaldaten eines Beschuldigten, aktenführende Behörde nebst Aktenzeichen und Zeitpunkt der Einleitung, Tatzeit und Tatort abrufbar sind.

bb. Probleme/ Grenzen

Schwierigkeiten, die sich bei der Arbeit der Ermittlungsbehörden im Umfeld von Fake-Shops ergeben, bestehen bspw. in einer erschwerten Ermittlung durch Zeitverlust, weil Geschädigte oft mehrere Wochen abwarten, ehe sie sich an die Polizei wenden. Viele Fake-Shop-Betreiber wechselten aber schnell auf andere Domains bzw. schalteten den bisherigen Shop ab.

Aus Sicht der Ermittlungsbehörden muss es das Ziel sein, Ermittlungen in Tatzeitnähe führen zu können, wenn noch Verbindungen zwischen den einzelnen operationellen Ebenen bestehen (Geldübergaben, Treffen, Telefonkontakte). Dadurch gäbe es zahlreiche weitere Ermittlungsansätze (Observation, GPS-Überwachung, TK-Überwachung etc.).

Weitere Schwierigkeiten ergeben sich durch nicht ausreichend geklärte Zuständigkeiten der Ermittlungsbehörden. Dies führt häufig zu weiteren Verzögerungen, die eine Rückverfolgung der Daten in die Vergangenheit erheblich erschweren.
Während grundsätzlich das Tatortprinzip gilt, bei Fake-Shops die Täter i.d.R. aber unbekannt sind, greift das Wohnortprinzip (Zuständigkeit nach Wohnort des Geschädigten). Häufig würden somit keine Sammelverfahren geführt, obwohl ein Fake-Shop an vielen Orten viele Opfer schädigt. Für die zentrale Steuerung spezifischer Konstellationen führen zudem die bei Fake-Shops im Regelfall falschen Personaldaten nicht weiter. Entscheidend wären dafür notwendig: Bezeichnung des Fake-Shops/Domain, Auflistung aller Ermittlungsdienststellen mit Aktenzeichen zu diesem Fake-Shop und, wenn schon ermittelt: Standort des Servers sowie Hinweis auf die Dienststelle der zentralen Bearbeitung.

Ein weiteres Problem stellt der Umstand dar, dass Fake-Shop-Betreiber häufig ausländische Provider nutzen, die anders als deutsche Provider meist nicht auf Löschanfragen reagieren.

Problematisch für die Rechts- und Strafverfolgung ist zudem die meist schwierige Identifizierung der Fake-Shop-Betreiber. Bei der Registrierung der .de-Domain gibt es keine Identitätsprüfung bzw. es müssen keine Dokumente bei der Registrierung vorgelegt werden. Es ist möglich, dass die Domaininhaber falsche Daten bei der Domain-Registrierung angeben. In einigen Fällen werden für die Registrierung von Domains auch Daten von anderen Webseitenbetreibern, die z.B. aus dem Impressum von Webseiten stammen, verwendet. Dieser Identitätsdiebstahl fällt oft erst auf, wenn Verbraucher, Verbraucherschutzorganisationen oder Ermittlungsbehörden die Webseitenbetreiber aufgrund nicht gelieferter Waren kontaktieren. Auch anhand der Daten, die beim Abschluss eines Vertrages mit einem Hosting-Provider anzugeben sind, ist die Identifizierung der Fake-Shop-Betreiber oftmals kompliziert, da auch dort gestohlene Identitäten zur Verschleierung eingesetzt werden. Eine Identitätsprüfung seitens der Hosting-Provider findet in der Regel nicht statt. Die Zwischenschaltung von teilweise mehreren Resellern erschwert zudem die Rückverfolgung der wahren Fake-Shop-Betreiber.

c. Löschung der Webinhalte durch Hosting-Provider

aa. Beschreibung

Die Zusammenarbeit zwischen Ermittlungsbehörde und Hosting-Provider gestaltet sich derzeit so, dass die jeweilige Ermittlungsbehörde mittels Whois-Abfrage bei der DENIC beziehungsweise durch spezielle Tools ein technisches Tracing der URL des in Verdacht stehenden Fake-Shops durchführt und damit ermittelt, wer verantwortlicher Hosting-Provider der Webseite ist und wo sich der Serverstandort befindet. Im Anschluss wendet sich die Ermittlungsbehörde an den so ermittelten Hosting-Provider mit einem Hinweis auf den strafrechtlich relevanten Tatbestand, der durch den Fake-Shop verwirklicht wird. Neben der Darlegung der Tatsachen des jeweiligen Falles, der Nennung der betroffenen URL und der verwirklichten Delikte beinhaltet dies meist Informationen über die Zahl der Geschädigten sowie den geschätzten bereits eingetretenen oder noch bevorstehenden Schaden. Damit verbunden ist in der Regel der Hinweis, dass der Hosting-Provider sich mit nunmehriger positiver Kenntnis des strafrechtlichen Sachverhalts, sollte er nicht unverzüglich eine Entfernung des Webseiteninhalts vornehmen (lassen), möglichen Regressansprüchen Dritter aussetze sowie sich unter Umständen der Beihilfe zum Betrug strafbar mache.

Kooperiert der Hosting-Provider, nimmt er Kontakt zum Domaininhaber auf, setzt ihn vom gemeldeten Sachverhalt in Kenntnis und fordert ihn zur Entfernung des Fake-Shops auf. Falls der Aufforderung nicht Folge geleistet wird, entfernt der Hosting-Provider den Inhalt selbst.

bb. Probleme/ Grenzen

Problematisch in der Zusammenarbeit der Ermittlungsbehörden mit den Hosting-Providern sind im Wesentlichen zwei Aspekte. Zum einen gibt es keine ausdrückliche Regelung, wann die Hosting Provider zur Löschung des Webseiteninhalts verpflichtet sind. Das Telemediengesetz (TMG) hilft insofern nicht weiter, als es selbst keine ausdrückliche Ermächtigungsgrundlage für eine Anordnungsbefugnis darstellt, sondern vielmehr eine solche voraussetzt. Das Fehlen einer konkreten Befugnis zur Anordnung gegenüber den Hosting-Providern (neben der Generalklausel in den Polizeiaufgabengesetzen der Länder) führt zu dem Problem, dass diese unterschiedlich schnell die Löschung des Webseiteninhalts veranlassen. Während manche Provider schon nach einem Telefonat und anschließendem Fax mit grober Sachverhaltsschilderung seitens der polizeilichen Ermittlungsbehörde tätig werden, fordern andere eine staatsanwaltliche Weisung beziehungsweise einen Beschlagnahmebeschluss nach §§ 94, 98 Strafprozessordnung (StPO). Dadurch bleiben bereits polizeilich bekannte Fake-Shops länger aktiv, was eine Erhöhung der Zahl geschädigter Verbraucher zur Folge haben kann.

Die Problemwahrnehmung der Ermittlungsbehörden in diesem Bereich ist nach Rückmeldung der angehörten Experten allerdings uneinheitlich.

Der zweite Themenkomplex betrifft die Fälle, in denen der Fake-Shop von einem Provider in einem anderen EU-Mitgliedstaat oder in einem Drittstaat gehostet wird. Kooperieren diese nicht auf freiwilliger Basis mit den anfragenden deutschen Ermittlungsbehörden, bleibt bislang nur der Weg über ein Rechtshilfeersuchen, das aber oftmals ebenfalls ohne Erfolg bleibt.

II. Geprüfte Maßnahmen zur besseren Bekämpfung von Fake-Shops

1. Präventive Maßnahmen

a. Verbesserung der Aufklärungsarbeit

Die Aufklärungs- und Präventionsarbeit insbesondere der Verbraucherverbände und der Polizei wird immer wieder auch gut von den Medien aufgegriffen, so dass sie eine sehr große Reichweite erzielt und gut wahrnehmbar ist. Sie stößt aber vor allem wegen der zunehmenden Perfektionierung der betrügerischen Webseiten immer wieder an Grenzen. Es handelt sich daher um eine kontinuierliche Aufgabe, bei der die Maßnahmen stetig an die sich verändernden Rahmenbedingungen angepasst werden sollten.

b. Einrichtung einer Meldestelle

aa. Beschreibung

Aus den Ergebnissen der Expertenrunde konnte die Schlussfolgerung gezogen werden, dass die Informationsflüsse und die Vernetzung verschiedener Institutionen ausbaufähig sind. Eine Bestandsaufnahme der bereits vorhandenen Strukturen hat ergeben, dass es auf Strafverfolgungsseite beispielsweise mit dem ZStV und auf Verbraucherseite mit dem Marktwächter Digitale Welt (s.o. B. I. 2. c) bereits Stellen gibt, die jeweils Daten und Fallzahlen in ihren Datenbanken und Registern vorhalten. Ein standardisierter und regelmäßiger Informationsaustauch zwischen den verschiedenen Institutionen erfolgt bislang nicht. Vor diesem Hintergrund wurde in der VSMK (Ziff. 4 des VSMK-Beschlusses) die Einrichtung einer bundesweit agierenden zentralen Meldestelle erwogen, die Informationen zu konkreten Fake-Shops bündelt und gegebenenfalls weiterverteilt.

bb. Bewertung

Angesichts der vorhandenen Strukturen und Potentiale erscheint die Errichtung einer zusätzlichen Meldestelle derzeit nicht erforderlich. Vielmehr ist es sinnvoll, zunächst die bestehenden Stellen mit dem Ziel einer beständigen Kooperation besser zu vernetzen.

Der Marktwächter Digitale Welt bündelt die eingehenden Verbraucherbeschwerden und Fallzahlen, arbeitet die Informationen zu Fake-Shops bereits umfassend auf und stellt diese den Verbraucherzentralen als interne Datenbank für ihre tägliche Arbeit zur Verfügung. Die hier zusammengeführten Hintergrundinformationen zu konkreten Fake-Shops könnten auch die bestehende Informationslage bei den Ermittlungsbehörden ergänzen und stärken. Zur schnellen und effektiven Bekämpfung des regelmäßig bundesweit relevanten Massenphänomens eines Fake-Shops, regt die Projektgruppe daher an, dass dem Marktwächter

Digitale Welt eine konkrete Ansprechstelle auf Ermittlungs- bzw. Strafverfolgungsseite benannt und damit ein regelmäßiger Informationsaustausch gefördert wird.

Die Anhörungen im Rahmen der Expertenrunde haben zudem ergeben, dass die Ermittlungsarbeit in den einzelnen Ländern sowie die Informationsflüsse zwischen den Stellen auf Strafverfolgungsseite zum Teil sehr unterschiedlich organisiert sind. Zur Koordination und zur effizienten Ausschöpfung der Informationen über Ländergrenzen hinweg, könnte eine zentrale Stelle auf Strafverfolgungsseite sinnvoll sein, bei der die Daten zu Fake-Shops und den Ermittlungsverfahren zusammengeführt und von den Ermittlungsbehörden abgefragt werden können.

c. Einrichtung einer Website (Liste)

aa. Beschreibung

Im Rahmen der Ziff. 5 des VSMK-Beschlusses stellte sich die Frage, ob mutmaßliche Fake-Shops nach vorangegangener Prüfung veröffentlicht werden könnten, um weitere Betrugsopfer dieser Fake-Shops auf Verbraucherseite zu verhindern.

Die bislang bestehenden Listen werden meist von Privatpersonen erstellt und gepflegt (z.B. www.onlinewarnungen.de). Da sie häufig durch private Spenden und Schaltung von Werbung finanziert werden, verschwimmen die Grenzen zwischen unabhängiger Verbraucheraufklärung und Werbeangeboten. Zudem sind Haftungsfragen weitgehend ungeklärt.

Deutlich weniger Websites werden öffentlich gefördert oder sogar von behördlicher Seite betrieben. Exemplarisch wurde das österreichische Projekt www.watchlist-internet.at befragt, das seit ca. fünf Jahren von einem privaten gemeinnützigen Verein betrieben und von der öffentlichen Hand gefördert wird (u.a. vom Bundesamt für Konsumentenschutz). Das Projekt ist bei der Schlichtungsstelle Internet Ombudsmann angegliedert und benötigt pro Jahr ein Budget von weniger als 100.000 Euro. Technisch werden Suchmaschinenoptimierung (SEO) und effiziente Schlagwortsetzung eingesetzt. Bei der Suche nach günstigen Onlineangeboten (z.B. für Handtaschen einer bestimmten Marke) wird den Verbraucherinnen und Verbrauchern über bzw. unter den aufgelisteten Shops die Website der Watchlist-Internet angezeigt. Auf diese Weise werden potentielle Fake-Shop Opfer darin

unterstützt, die Seriosität eines Onlineshops kritisch zu hinterfragen und die Website von Watchlist-Internet statt die des Fake Shops anzuklicken.

Die Website informiert Verbraucherinnen und Verbraucher mit möglichst einfachen Erklärungen über das Phänomen Fake Shops und darüber, wie sie diese eigenständig identifizieren können. Auf der Website werden nur solche Shops gelistet, die nach einem internen Kriterienkatalog sicher als Fake-Shops eingestuft werden können. Bestehen geringste Zweifel an der Einordnung, unterbleibt eine Veröffentlichung des möglicherweise nur schlecht betreuten, aber seriösen Shops. Aus diesem Grund, so gibt es das Projekt an, habe es bisher keinen Haftungsfall und keinen Rechtsstreit mit gelisteten Shops gegeben.

Mit dem Einsatz der SEO habe das Projekt gute Erfahrungen gemacht. Es wird geschätzt, dass ca. 75 % der Website-Besucher über die SEO und ca. 25 % über den Newsletter des Projekts auf die Seite gelangen.

bb. Bewertung

Angesichts des Erfolgs des österreichischen Projekts Watchlist Internet erscheint die Einrichtung eines Pilotprojekts beim Marktwächter Digitale Welt sinnvoll. Denn dort besteht neben einem umfangreichen Wissensstand bezüglich aktueller Fake-Shops auch eine Aufgabenzuständigkeit bezüglich der Warnung und Aufklärung von Verbraucherinnen und Verbrauchern über dieses Phänomen. Dabei sollte ein entsprechendes Pilotprojekt über einen Zeitraum von ein bis zwei Jahren unter entsprechender Förderung eingerichtet und anschließend evaluiert werden.

Voraussetzung für eine einheitliche Einstufung als Fake-Shop ist die vorherige Aufstellung eines nachvollziehbaren Kriterienkatalogs durch den Marktwächter Digitale Welt.

Zwar kann bei Nichtlistung eines Shops im Umkehrschluss der Eindruck bei den Verbraucherinnen und Verbrauchern entstehen, dass es sich nicht um einen Fake-Shop handelt. Das Projekt Watchlist Internet hat diesbezüglich aber darauf hingewiesen, dass der Liste der Hinweis der (naturgemäßen) Unvollständigkeit vorgeschaltet ist. Im Gegensatz zu der bisherigen Informationslage, nach der Verbraucherinnen und Verbraucher mühsam selbst z.B. in Foren nach der Bewertung eines bestimmten Shops suchen müssen, werden beim Besuch der Website mit der Liste auch Informationen zum eigenständigen Erkennen von

Fake-Shops gegeben. Dadurch steigt die Wahrscheinlichkeit, dass die Verbraucherinnen und Verbraucher auch bei Nichtlistung eines Fake-Shops diesen als solchen einstufen können.

Haftungsrisiken können zwar für den Fall bestehen, dass ein Shop fälschlicherweise als Fake-Shop eingestuft und veröffentlicht wird. Dem kann jedoch dadurch wirksam begegnet werden, dass die Veröffentlichung als Fake-Shop nur bei absolut eindeutiger Einstufung erfolgt. Es besteht zudem die Möglichkeit, die aufgelisteten Shops nicht explizit als Fake-Shops zu bezeichnen, sondern die Verbraucherinnen und Verbraucher darauf hinzuweisen, dass Zweifel an der Seriosität der genannten Shops bestehen und daher zu besonderer Vorsicht geraten wird.

Werden gelistete „.de-Domains“ gelöscht, ist zu prüfen, ob diese auf der Webseite verbleiben sollen. Für Nutzer, die unter dieser Internetadresse bestellt hatten, kann die Information, dass es sich um einen Fake Shop handelte, wichtig sein. Zum anderen muss bedacht werden, dass die Domain jederzeit an einen anderen Domaininhaber vergeben werden könnte, der unter dieser Internetadresse möglicherweise einen seriösen Onlineshop betreiben möchte; der Domaininhaber könnte dann gegen die Veröffentlichung auf der Webseite vorgehen wollen. Es wird angeregt, dass der Marktwächter Digitale Welt Lösungen dazu erarbeitet bzw. gegebenenfalls verschiedene Kennzeichnungsoptionen (z.B. Screenshot der Startseite des Fake-Shops neben dem Link) durchspielt und evaluiert.

d. Identitätsprüfung im Domain-Registrierungsprozess der DENIC

aa. Beschreibung

Ausgehend von der Prüfbitte zu Regelungen in Bezug auf Domains (Ziffer 5 des VSMK-Beschlusses) hat sich die Projektgruppe mit dem Registrierungsprozess der Top Level Domain „.de“ befasst. Bei einer Webseite mit der Top Level Domain „.de“ wird von vielen Nutzern davon ausgegangen, dass der Standort des Shops in Deutschland ist. Nach Angaben der DENIC sind derzeit ca. 16,2 Millionen Domains mit der Endung „.de“ registriert, was einen Marktanteil in Deutschland von 61,4 Prozent ausmacht.

Für Internetnutzer ist diese länderspezifische Top Level Domain mit eindeutigem geografischen Bezug zumindest ein Hinweis, dass es einen Zusammenhang des Web-Shops mit Deutschland gibt. Daher kann davon ausgegangen werden, dass das Vertrauen der Nutzer

in die Einhaltung von bestimmten Standards hoch ist. Auch als „Aushängeschild“ für Deutschland spielt diese TOP Level Domain eine Rolle.

In Deutschland findet bei der Vergabe einer „.de-Domain“ durch die DENIC bisher keine Identitätsprüfung statt.

In einer Untersuchung des Marktwächters Digitale Welt (Fake-Shops – Wie frühere Domaininhaber zu vermeintlichen Betreibern von Fake-Shops werden, Hintergrundpapier August 2018) wurde u.a. das Registrierungssystem in Dänemark betrachtet. Demnach erfolgt die Domain-Registrierung in Dänemark mit Identitätsprüfung. In den meisten Fällen wird die Registrierung über einen Registrar vorgenommen. Aufgrund einer gesetzlichen Verpflichtung überprüft die Registrierungsstelle die Identität des späteren Domaininhabers vor Domain-Freigabe. Bei dänischen Bürgern bzw. Unternehmen erfolgt der Abgleich mit der Steuerpersonennummer bzw. dem Handelsregister. Handelt es sich um eine nicht in Dänemark gemeldete Person bzw. Unternehmen, wird eine Risikoeinschätzung vorgenommen und ggf. nach Identitätsnachweisen gefragt. Bei falschen Daten kann die Registrierungsstelle die Registrierung aufheben.
Nach den Erkenntnissen des Marktwächters Digitale Welt ist der Anteil der betrügerischen Webseiten mit Fake-Shops in Dänemark nach Einführung einer Identitätsprüfung im Netz von 6% auf 1% gesunken (vgl. auch Analyse des DIFO / DK Hostmaster unter https://www.dk-hostmaster.dk/sites/default/files/2018-04/DIFOs-indsats-for-at-begraense-kriminaliteten-med-brug-af-dk-domaenenavne_onepager_EN_0.pdf). Das in Dänemark geltende Registrierungssystem könnte nach Auffassung des Marktwächters Digitale Welt als Vorlage für eine Änderung des deutschen Registrierungsprozesses herangezogen werden.

Eine Identitätsprüfung bei der Vergabe einer „.de-Domain“ müsste in den bestehenden Registrierungsprozess integriert werden. Dabei könnte sich die DENIC auch an bereits existierenden Verfahren orientieren, die beispielsweise bei der Einrichtung eines Bankkontos oder beim Kauf von Prepaid-SIM-Karten üblich sind.

bb. Bewertung

Die Einführung einer Identitätsprüfung im Domain-Registrierungs-Prozess der DENIC ist aus Sicht der Projektgruppe vor dem Hintergrund der Erfahrungen aus Dänemark eine wirksame Maßnahme gegen Fake-Shops.
Jedenfalls kann damit die Registrierung von Domains unter einer falschen bzw. gestohlenen Identität stark erschwert werden. Dies lässt vermutlich die Anzahl der Fake-Shops unter einer „.de-Domain“ erheblich zurückgehen.

Eine Übertragung des Systems aus Dänemark, in dem ein Abgleich mit der Steuerpersonennummer erfolgt, bietet sich in Deutschland eher nicht an, da diese Nummer eine andere Zweck- und Nutzerbestimmung hat. Jedoch gibt es verschiedene, bereits in anderen Bereichen genutzte Identifizierungsverfahren, die verwendet werden könnten. Dabei erfolgt die Überprüfung der Identität zum Beispiel über Post-Ident oder Videochat. Auch bei ausländischen Personen oder Unternehmen könnten entsprechende Verfahren genutzt werden.

Die Bedenken gegen die Einführung einer Identitätsprüfung sind aus Sicht der Projektgruppe nicht durchgreifend. Auch bisher ist die Registrierung einer „.de-Domain“ nicht ohne Angabe von Daten möglich. Das Registrierungsverfahren, in dem spätere Domaininhaber bereits jetzt ihre Identität offenlegen müssen (u.a. Name und Anschrift), wird lediglich um eine Prüfung dieser Identität ergänzt. Grundsätzlich wird eine Identitätsprüfung mehr Aufwand und Zeit auch für private Nutzer bedeuten, die zum Beispiel eine Domain registrieren, um eine private Webseite ohne Shop zu betreiben. Dem gegenüber steht jedoch der Vorteil für alle Internetnutzer, dass strafrechtliche Handlungen unterbunden bzw. verfolgt werden können. Ein wesentlicher Rückgang der Fake-Shops unter der „.de-Domain“ wäre für alle seriösen Akteure ein Gewinn.

2. Repressive Maßnahmen

a. Spezielle Anordnungsbefugnis für Polizeibehörden zur Löschung des Webseiteninhalts

aa. Beschreibung

Geprüft wurde von der Projektgruppe die Möglichkeit, einen Spezialtatbestand in die Polizeigesetze (PAGs) der Länder einzuführen, der unter besonderer Beachtung des Verhält-

nismäßigkeitsgrundsatzes eine Befugnis der polizeilichen Ermittlungsbehörden gegenüber den Hosting-Providern zur Löschungsanordnung regelt. Auf Grundlage dieser spezielleren Anordnungsbefugnis der Polizei wäre der Hosting-Provider zur Entfernung des Webseiteninhalts verpflichtet. Nach Aussagen von Teilen der angehörten Experten wird aber angesichts der von dem betrügerischen Angebot auf der Webseite ausgehenden Gefahr, die Voraussetzung für eine notwendige Maßnahme seitens der Polizei zur Abwehr einer (konkreten) Gefahr für die öffentliche Sicherheit oder Ordnung ist, die allgemeine Generalklausel zur Gefahrenabwehr für ausreichend angesehen.
Auch eine freiwillige Vereinbarung zwischen den Hosting-Providern und den Ermittlungsbehörden beziehungsweise einer Selbstverpflichtung der Hosting-Provider als milderes Mittel zu einer gesetzlichen Regelung wurde untersucht. Diese könnte vorsehen, dass sich der Provider verpflichtet, nach Mitteilung der jeweils ermittelnden Polizeibehörde unverzüglich auf die Entfernung des Webseiteninhalts hinzuwirken.
Für den zweiten Problemkreis der ausländischen Provider wird die Notwendigkeit einer Verknüpfung mit der Frage der Löschverpflichtung der DENIC (wie in B. II. 2 b erläutert) gesehen.

bb. Bewertung

Aus Sicht der angehörten Experten ist die Löschung der Webseiten-Inhalte mit den derzeit vorhandenen Mitteln grundsätzlich und in den meisten inländischen Fällen ein schneller und technisch gut umsetzbarer Weg, um gegen Fake-Shops vorzugehen. § 7 III S. 1 TMG legt ausdrücklich eine Verpflichtung des Diensteanbieters aufgrund gerichtlicher oder behördlicher Anordnung fest. Eine solche Anordnungsbefugnis könnte grundsätzlich für polizeiliche Behörden in den Generalklauseln der Länder gesehen werden und wird größtenteils als rechtliches Instrumentarium als ausreichend bewertet. Eine konkrete Empfehlung für die Schaffung einer Spezialbefugnisnorm kann daher derzeit nicht ausgesprochen werden.

Problematisch an einer Vereinbarung zwischen den Hosting-Providern und den polizeilichen Ermittlungsbehörden sowie auch an einer Selbstverpflichtung ist die unüberschaubare Vielzahl inländischer Hosting-Provider, die es kaum möglich erscheinen lässt, alle relevanten Hosting-Provider mit einzuschließen und somit der Zielsetzung einer konsequenten und einheitlichen Vorgehensweise gegen Fake-Shops gerecht zu werden.

b. Löschen einer registrierten „.de-Domain“

aa. Beschreibung

Durch Löschung einer Domain wird erreicht, dass eine Webseite nicht mehr über diese Internetadresse abrufbar ist. Wird eine gelöschte Domain zum Beispiel über den Webbrowser eingegeben, führt die Verbindung ins Leere. Der Inhalt einer Webseite wird dadurch nicht gelöscht. Die Webseite ist weiterhin über die IP-Adresse zugänglich und kann jederzeit über eine andere registrierte Domain für alle Internetnutzer zugänglich gemacht werden.

Die Löschung einer „.de-Domain“ ist derzeit auf folgenden Wegen möglich:

- Antrag des Domaininhabers bzw. seines Vertreters,
- Beanstandung von Dritten, dass der Domain-Name Recht verletzt und dies gerichtlich festgestellt wurde oder dies offenkundig und ohne weiteres feststellbar ist (z.B. bei Verwendung offizieller Bezeichnungen von Regierungen durch Private, vgl. BGH Urteil vom 27.10.2011 I ZR 131/10),
- Löschung durch DENIC aufgrund der vertraglichen Grundlagen, zum Beispiel aufgrund fehlender Zahlung durch den Domaininhaber.

Das Löschen einer „.de-Domain“ erfolgt zunächst vorläufig. Um Domaininhaber vor einer versehentlichen Löschung der Domain zu schützen, gilt bei „.de-Domains“ ein Karenzverfahren, d.h. während einer 30-tägigen sogenannten Redemption Grace Period kann eine zuvor gelöschte Domain nur im Auftrag ihres vormaligen Domaininhabers erneut registriert werden.

Die Löschung einer Domain könnte zukünftig insbesondere für die Fälle eingeführt werden, in denen keine Löschung der Webseite über den Hosting-Provider möglich bzw. Erfolg versprechend ist (siehe B. II. 2. a. bb) und in denen Behörden die DENIC dazu auffordern.

bb. Bewertung

Die Löschung einer „.de-Domain“, die auf einen Fake-Shop führt, kann einen erheblichen Beitrag zur Bekämpfung des Fake Shops leisten, sollte aber nur dann eingesetzt werden, wenn andere und effizientere Maßnahmen zur Löschung der Inhalte nicht greifen. Wenn keine Löschung über den Hosting-Provider möglich bzw. Erfolg versprechend ist, kann die Löschung einer Domain den Zugang zu der Webseite jedenfalls erheblich einschränken.

Denn es ist unwahrscheinlich, dass Internetnutzer durch die Eingabe der IP-Adresse auf den Fake-Shop gelangen.

Voraussetzung für das Löschen einer „.de-Domain“ eines Fake-Shops müssten klare, eindeutige Kriterien für die Löschung sein, die bei Verdacht auf Fake-Shops leicht und zweifelsfrei geprüft werden könnten. Der im Zusammenhang mit der Einrichtung einer Webseite zu erstellende Kriterienkatalog (siehe B. II. 1. c. bb) könnte hierfür genutzt werden. Eine Kooperation zwischen Ermittlungsbehörden, dem Marktwächter Digitale Welt und der DENIC ist sinnvoll, um die Löschung im Kontext mit den anderen Maßnahmen, die in Bezug auf den Fake-Shop unternommen werden, abzustimmen. Auch eine klare Beschreibung der Prüfschritte und Konsequenzen sowie eine Einbeziehung in die vertragliche Ausgestaltung der Domainregistrierung durch die DENIC ist aus Sicht der Projektgruppe von Vorteil. Die DENIC könnte sich verpflichten, nach einer Meldung eines Fake Shops durch eine Ermittlungsbehörde im Sinne eines „notice and take domain down“-Verfahrens die Domain zu löschen.

Zur Vermeidung von Schadensersatzforderungen von möglicherweise unberechtigt betroffenen Domaininhaber bzw. Shop-Betreiber müsste klar geregelt werden, wie in Zweifelsfällen zu verfahren ist. Eine gerichtliche Entscheidung sollte aufgrund der langen Verfahrenszeiten nur im Ausnahmefall abgewartet werden müssen.

c. CPC-VO

aa. Beschreibung

In der CPC-Verordnung, die ab 17. Januar 2020 anwendbar sein wird und die bisherige Verordnung (EG) 2006/2004 ablöst, ist erstmals eine umfassende behördliche Befugnis aufgenommen, Inhalte von Online-Schnittstellen zu entfernen, zu beschränken oder einen Warnhinweis beim Zugriff auf diese anzeigen zu lassen und hierzu Anordnungen gegenüber Anbietern von Hosting-Diensten, Registern oder Registrierungsstellen für Domänenamen auszusprechen.

Die neu geschaffene Befugnis in Artikel 9 Absatz 4 Buchstabe g) gibt den zuständigen CPC-Behörden erstmals eine Rechtsgrundlage dafür, Inhalte von Online-Schnittstellen selbst zu entfernen, zu beschränken oder anzuordnen, dass ein ausdrücklicher Warnhinweis zu platzieren ist (Artikel 9 Absatz 4 Buchstabe g) i), gegenüber Anbietern von

Hosting-Diensten die Entfernung, Sperrung oder Beschränkung des Zugangs zu einer Online-Schnittstelle anzuordnen (Artikel 9 Absatz 4 Buchstabe g) ii) oder gegebenenfalls gegenüber Registern oder Registrierungsstellen für Domänennamen die Entfernung eines vollständigen Domänennamens und die Gestattung der Registrierung der betreffenden zuständigen Behörde anzuordnen (Artikel 9 Absatz 4 Buchstabe g) iii). Voraussetzung für die Anwendbarkeit der CPC-Verordnung ist das Vorliegen eines „Verstoßes innerhalb der Union“. Hierunter fällt nach Artikel 3 Nr. 2 der CPC-Verordnung jede Handlung oder Unterlassung, die gegen „Unionsrecht zum Schutz der Verbraucher“ verstößt und die Kollektivinteressen von Verbrauchern geschädigt hat, schädigt oder voraussichtlich schädigen kann, die in einem anderen Mitgliedstaat oder anderen Mitgliedstaaten als dem Mitgliedstaat ansässig sind, in dem die Handlung oder Unterlassung ihren Ursprung hatte oder stattfand, der für die Handlung oder Unterlassung verantwortliche Unternehmer niedergelassen ist, oder Beweismittel oder Vermögensgegenstände des Unternehmens vorhanden sind, die einen Zusammenhang mit der Handlung oder Unterlassung aufweisen. Als „Unionsrecht zum Schutze der Verbraucher" gelten nach der CPC-Verordnung nur die im Anhang aufgeführten Verordnungen und Richtlinien. Erforderlich nach Artikel 3 Nr. 2 der CPC-Verordnung ist zudem, dass der Verstoß grenzüberschreitend ist, also Verbraucher und Unternehmer in verschiedenen Mitgliedstaaten ihren Wohnsitz oder ihre Niederlassung haben bzw. der begangene Verstoß seinen Ursprung in einem anderen Mitgliedstaat hatte oder stattfand. Somit unterfallen alle Verstöße, die von Unternehmern außerhalb der EU begangen werden, nicht dem Anwendungsbereich der CPC-Verordnung.

bb. Bewertung

Neben der grundsätzlichen Eröffnung des Anwendungsbereichs der CPC-Verordnung (siehe hierzu obige Ausführungen zum „Verstoß innerhalb der Union“) setzt die Ausübung dieser Befugnis allerdings zusätzlich voraus, dass keine anderen wirksamen Mittel zur Verfügung stehen, um die Einstellung des Verstoßes zu bewirken und durch die jeweilige Maßnahme das Risiko einer schwerwiegenden Schädigung der Kollektivinteressen von Verbraucherinnen und Verbrauchern verhindert wird. Diese zusätzlichen Voraussetzungen schränken den Anwendungsbereich nicht unerheblich ein. Zum einen reicht nicht jede Schädigung der Kollektivinteressen von Verbraucherinnen und Verbrauchern aus, sondern diese muss schwerwiegend sein. Dem in Rede stehenden Verstoß dürfte daher jedenfalls eine gewisse Bedeutung zukommen müssen. Zum anderen dürfen aber auch keine anderen wirksamen Mittel zur Verfügung stehen, um die Einstellung des Verstoßes zu erreichen. Diese weitere Beschränkung des Anwendungsbereichs geht noch weiter als der oh-

nehin einzuhaltende Verhältnismäßigkeitsgrundsatz, der unter anderem die Erforderlichkeit einer Maßnahme verlangt, also, dass es sich bei mehreren gleich wirksamen Mitteln um das mildeste Mittel handeln muss. Die CPC-Verordnung stellt hingegen nicht auf die Milde eines Mittels ab, sondern setzt vielmehr voraus, dass keine anderen wirksamen Mittel zur Verfügung stehen.

Für die behördliche Praxis ist naheliegend, dass bei Hosting von Inhalten im Inland Anordnungen an die Hosting-Provider gerichtet und durchgesetzt werden können. Außerdem dürften Maßnahmen, die auf die Entfernung eines vollständigen Domänennamens (Artikel 9 Abs. 4 Buchstabe g iii) und damit auf die Unterbrechung der Zuordnung von Domänenamen zu IP-Adressen zielen, eine erhebliche Wirksamkeit entfalten. Verbraucher sind an legalen Inhalten interessiert und wollen eine Seite in aller Regel nur unter einem Domänenamen aufsuchen. Wenn dieser nicht mehr funktioniert oder auf einen staatlichen Warnhinweis umgeleitet wird, wird das Interesse am Aufsuchen der Webseite in aller Regel entfallen. Insoweit dürften Anordnungen, die sich an im Inland gelegene Instanzen des DNS-Systems (bestehend aus Serverinstanzen und Registrierungsstellen) richten, naheliegen.

Darüber hinaus ist darauf hinzuweisen, dass Fälle die ihrem Schwerpunkt nach strafrechtlichen Charakter haben, nach bisheriger Praxis in dem Netzwerk in der Regel nicht durch die Verbraucherschutzbehörden des CPC-Netzwerks bearbeitet werden, sondern den Strafverfolgungsbehörden überlassen werden. In Deutschland besteht bei der Verfolgung einer Ordnungswidrigkeit sogar eine Verpflichtung, das Verfahren in diesem Fall der Staatsanwaltschaft zur näheren Prüfung vorzulegen (§ 41 Absatz 1 OWiG).

C. Empfehlungen

Die Untersuchungsergebnisse des Marktwächters Digitale Welt von August 2018 bestätigen die Ausweitung des Problems der Fake-Shops im Internet. Neben der wachsenden Anzahl von Fake-Shops, wurde festgestellt, dass deren Aktivitäten vielfältiger und variantenreicher werden. Jeder vierte der befragten Internet-Nutzer in Deutschland hat mindestens einmal bestellte und bezahlte Ware nicht erhalten. Bei über vier Millionen der Betroffenen wird von einem Betrug durch Fake-Shops ausgegangen. Die Folge sind nicht nur die materiellen Schäden, sondern auch eine erhebliche Verunsicherung der Verbraucherinnen und Verbraucher~~n~~ bei der Nutzung des Online-Handels.

Sowohl im präventiven als auch im repressiven Bereich bestehen Ansatzpunkte, um das Problem der Fake-Shops effektiver zu bekämpfen.

Die bestehende kontinuierliche Aufklärungs- und Präventionsarbeit durch die Verbraucherzentralen der Länder und die Polizeibehörden wird durch die Informationstätigkeit der Medien gut ergänzt, sodass bereits eine sehr große Reichweite erzielt wird. Angesichts der zunehmenden Perfektionierung der betrügerischen Webseiten ist es jedoch erforderlich, die Informationstätigkeit sowie die Informationskanäle stetig anzupassen.

Der Aktionsbereich eines Fake-Shops ist in der Regel nicht ortsgebunden, sondern erstreckt sich auf das gesamte Bundesgebiet und schädigt regelmäßig bundesweit Verbraucherinnen und Verbraucher. Dies führt dazu, dass häufig in mehreren Bundesländern Ermittlungen parallel geführt werden. Hierbei wird länderspezifisch unterschiedlich vorgegangen und das Phänomen Fake-Shop teilweise nicht in jeder Organisationseinheit einheitlich behandelt. Im Interesse einer effizienten Ermittlungsarbeit gilt es, die Informationsflüsse zwischen und innerhalb der einzelnen Institutionen zu verbessern und die Arbeitsprozesse bei den Ermittlungsbehörden und den Verbraucherzentralen der Länder zu vernetzen.

Auf Ebene der polizeilichen Ermittlungstätigkeit ist zum einen eine bessere Vernetzung des Staatsanwaltschaftlichen Zentralregisters (ZStV) mit anderen Ermittlungsbehörden bzw. polizeilichen Stellen eine Stellgröße. Zum anderen könnte gegebenenfalls zur Koordination und effizienten Ausschöpfung der Informationen über Ländergrenzen hinweg eine zentrale Stelle auf Strafverfolgungsseite sinnvoll sein, bei der die Daten zu Fake-Shops und den Ermittlungsverfahren zusammengeführt und von den Ermittlungsbehörden abgefragt werden können.

Die durch den Marktwächter Digitale Welt gebündelten Verbraucherbeschwerden und Hintergrundinformationen stehen den Verbraucherzentralen für ihre tägliche Arbeit als interne Datenbank zur Verfügung. Eine systematische Übersendung an Ermittlungsbehörden erfolgt bislang nicht, da dem Marktwächter in der Regel nicht bekannt ist, ob gegen einen Fake-Shop ermittelt wird und welche Staatsanwaltschaft diese Ermittlungen führt. Um die Arbeitsprozesse bei den Ermittlungsbehörden und den Verbraucherzentralen der Länder effizienter gestalten zu können, regt die Projektgruppe eine Kooperation zur Förderung des Informationsflusses und des regelmäßigen Austausches an. Hierzu bietet es sich an, dass

für den Marktwächter Digitale Welt zunächst bei dem ZStV ein konkreter Ansprechpartner benannt wird. Die Errichtung einer zusätzlichen bundesweit einheitlichen Meldestelle erscheint angesichts der Potentiale bei den vorhandenen Strukturen und Institutionen zunächst nicht notwendig.

Um das Erkennen von Fake-Shops auch für Verbraucherinnen und Verbraucher zu erleichtern, wird der Marktwächter Digitale Welt gebeten, ähnlich dem österreichischen Projekt www.watchlist-internet.at Informationen zum Thema Identifizierung von Fake-Shops und eine Webseite mit einer Auflistung derjenigen Online-Shops zu veröffentlichen, die nach einem internen Kriterienkatalog zweifelsfrei als Fake-Shops eingestuft werden können.

In einer Untersuchung stellte der Marktwächter Digitale Welt fest, dass ein erheblicher Teil der in Deutschland aufrufbaren Fake-Shops über eine „.de Domain“ verfügt. Webseiten mit der Endung „.de“ gelten bei den Verbraucherinnen und Verbrauchern in Deutschland als besonders vertrauenswürdig und suggerieren ein hohes Schutzniveau, das tatsächlich jedoch nicht gewährleistet ist. Aus Sicht der Projektgruppe ist daher die Einführung einer Identitätsprüfung im Domain-Registrierungsprozess der DENIC eine wirksame Maßnahme, um die Hürde für die Registrierung von Fake-Shops zu erhöhen. Die Erfahrungen aus Dänemark haben gezeigt, dass eine Identitätsprüfung zu einem Rückgang der Anzahl an Fake-Shops führen kann.

Aus Sicht der angehörten Expertinnen und Experten ist die Löschung der Webseiten-Inhalte grundsätzlich ein schneller und technisch gut umsetzbarer Weg, um gegen Fake-Shops vorzugehen. Es wurde jedoch festgestellt, dass die Löschung der Webseiteninhalte durch die Hosting-Provider trotz Aufforderung seitens der Behörden und Hinweise von Verbraucherseite nicht immer erfolgt. In solchen Fällen, in denen die Löschung der Webinhalte über die Hosting-Provider nicht möglich oder nicht erfolgsversprechend ist, bietet die Löschung der Domain eine wirksame Alternative, um die Erreichbarkeit eines Fake-Shops zumindest zu erschweren. Für die Löschung von Fake-Shop-Webseiten bzw. der betreffenden Domians müssen klare und eindeutige Kriterien vorliegen, wann es sich um einen zu löschenden Fake-Shop handelt. Die DENIC könnte sich verpflichten, nach einer Meldung eines Fake Shops durch eine Ermittlungsbehörde oder durch die Meldestelle im Sinne eines „notice and take domain.down“-Verfahrens die Domain zu löschen.

D. Anhang - Rolle der technischen Akteure beim Einrichten eines Onlineshops

Es existieren sehr unterschiedliche technische Möglichkeiten, einen Onlineshop auf einer Webseite, die nicht zu einer Onlineplattform gehört, einzurichten und diesen für Verbraucherinnen und Verbraucher erreichbar zu machen. Dies gilt ebenso für Fake-Shops. Im Folgenden wird grob skizziert, welche Akteure neben dem Webseitenbetreiber üblicherweise beim technischen Einrichten eines Onlineshops eine Rolle spielen.

Provider

Zu unterscheiden ist zwischen Hosting-Providern und Internet Service Providern.

Hosting-Provider sorgen dafür, dass der vom Kunden gewünschte Internetauftritt öffentlich verfügbar ist. Es können Reseller dazwischengeschaltet sein. Hosting-Provider haben direkten Zugriff auf den Serverinhalt und können die Löschung des Webseiteninhalts vornehmen, wodurch dieser Inhalt über die Internetadresse nicht mehr verfügbar ist. Üblicherweise ist zum Abschluss eines Hosting-Provider-Vertrags die Angabe von Namen, Adresse, E-Mail-Adresse, Telefonnummer und Bankverbindung notwendig. Die Richtigkeit der Angaben muss der Kunde bei Abschluss bestätigen. Eine Überprüfung findet über das Versenden eines Freischaltcodes an die angegebene Mobilfunknummer beziehungsweise E-Mail-Adresse statt. Ein Identitätsnachweis ist nicht erforderlich.

Internet Service Provider können zwar auch beispielsweise durch DNS-Sperren dafür sorgen, dass bestimmte Webseiten nicht mehr verfügbar sind. Allerdings sind die gesperrten Webseiten in diesem Fall – anders als bei Löschungen durch Hosting-Provider – nur für die Kunden des jeweils sperrenden Internet Service Providers gesperrt, für Kunden anderer Internet Service Provider jedoch nicht. Aus diesem Grund sind sie nach derzeitigem Stand nicht eingebunden in die Bekämpfung der Fake-Shops.

Domaininhaber und Registrierungsstelle

Über die Registrierung einer Domain wird erreicht, dass der Onlineshop eine leicht verständliche Adresse erhält.
Denn die Kommunikation zwischen Computern im Internet erfolgt über sogenannte IP-Adressen mit festgelegten langen Ziffernfolgen. Um für Internetnutzer die Bezeichnung von Internetadressen leichter zu machen und um eigene Internetadressen selbst bestimmen zu

können, wurde das Domain Name System entwickelt. Eine Domain ist somit eine Internetadresse.

Die Domainverwaltung unterscheidet sich je nach Land und Domain.
Die Domain-Endung „.de“ ist die länderspezifische Top-Level-Domain der Bundesrepublik Deutschland. Die Top-Level-Domain „.de“ wird von der DENIC eG mit Sitz in Frankfurt am Main verwaltet, d.h. dort werden Domains mit dieser Endung registriert.

In Bezug auf die Verwaltung bzw. Registrierung der „.de“-Domains existieren keine gesetzlichen Regelungen. Das Verfahren der Registrierung ist wie bei einem IT Dienstleister zertifiziert.
Der Hauptteil der Registrierungen erfolgt über Registrare. Es ist jedoch auch eine direkte Registrierung bei der DENIC möglich. Die Registrierung erfolgt nach dem Prinzip “first come first serve“ und hat grundsätzlich keine zeitliche oder anzahlmäßige Begrenzung. Eine gelöschte Domain kann wieder neu registriert werden.

Nach Angabe der DENIC ist die Registrierung ein rein technischer Vorgang. Es handelt sich um ein vollautomatisiertes Registrierungssystem über elektronische Schnittstellen. Folgende Daten müssen im Registrierungsprozess angegeben werden: Name bzw. Firma, Adresse (mit Stadt, Land und PLZ) sowie eine E-Mail-Adresse. Die Daten des Domaininhabers werden in der Regel über den Registrar an die DENIC übermittelt. Die DENIC prüft bei der Registrierung nicht, ob die Daten richtig sind. Es findet keine Identitätsprüfung statt. Der Registrierungsauftrag erfolgt über ein assistiertes Online-Formular mit Plausibilitätsprüfungen. Nach vollständigem Ausfüllen des Online-Formulars wird der Domainregistrierungsauftrag als PDF für den Antragsteller bereitgestellt. Der Auftrag ist dann rechtsverbindlich zu unterschreiben und an die DENIC zu senden. Danach wird die Registrierung vorgenommen. In Bezug auf die Registrierung über einen Registrar gibt es folgende Vertragsverhältnisse:

- Vertrag zwischen der Registrierungsstelle DENIC mit dem Registrar
- Vertrag zwischen der DENIC und dem Domaininhaber
- Vertrag zwischen Registrar und Domaininhaber.

Inhalt des Vertrages zwischen DENIC und dem Domaininhaber ist die Bereitstellung der technischen Funktion der Domain gegen Bezahlung. Die DENIC kann den Vertrag kündigen, wenn Folgendes eintritt:

- wenn Daten falsch sind,
- wenn nicht bezahlt wird,
- wenn offenkundig Rechte Dritter verletzt werden (nur den Domain-Namen betreffend, z.B. Markenrechte).

E. Glossar

DENIC - Die DENIC ist eine neutrale und nicht gewinnorientierte Gesellschaft mit Sitz in Frankfurt/Main, die als Registrierungsstelle für Domains mit der Endung „.de“ agiert. Die derzeit 295 Mitglieder der DENIC sind größtenteils Registrare unterschiedlicher Größe und Art.

Registrar – Ein Provider, der für den Domaininhaber die Domain bei der DENIC registriert. Dies kann auch der Provider sein, der die Webseite hostet (Hosting-Provider).

Domaininhaber – Natürliche Person oder juristische Person (z.B. Unternehmen), die die Domain registriert hat.

Hosting-Provider stellen für ihre Kunden üblicherweise gegen Bezahlung Webspace bereit und gewährleisten die Unterbringung von Webseiten auf dem Webserver eines Internet Service Providers (= Zugangsanbieter).

Internet Service Provider ermöglichen ihren Kunden, den Internetnutzern, mittels technischer Vorrichtungen den Transfer von IP-Paketen in und aus dem Internet, mithin Internetkonnektivität.

Domain – Internetadresse, die nach dem Domain Name System erstellt und registriert wird und auf eine bestimmte IP-Adresse bezogen ist. Sie ist in unterschiedliche Bestandteile eingeteilt. Die Domain-Endung, das Kürzel nach dem Punkt (.com oder .de), wird Top Level Domain genannt. Diese zeigt an, ob eine Internetpräsenz hauptsächlich in einem bestimmten Land oder einer bestimmten Stadt oder zu einem bestimmten Zweck, z.B. Information (.info), bzw. Themenbereich (.shop) auftritt. Der Teil vor dem Punkt wird Second Level Domain genannt. Eine Domain darf weltweit nur einmal registriert werden.

Webseite – Internetauftritt einer privaten oder juristischen Person im World Wide Web, der durch einen Browser über eine Domain für Internetnutzer abrufbar ist. Eine Webseite besteht zumeist aus mehreren HTML-Dateien, die zum Beispiel auf einem Webserver eines Hosting-Providers abgelegt sind.