

## E. Konterreaktion: Maßnahmen zur Umgehung der Verhinderung

Es verwundert kaum, dass die im vorigen Abschnitt beschriebenen Reaktionen der Webseitenbetreiber ihrerseits Konterreaktionen heraufbeschwören. Denn Nutzer, die sich von der verbreiteten Werbung im Internet bereits belästigt fühlen und aus freier Entscheidung, ein technisches Mittel zur Ausschaltung dieser Werbung einsetzen, werden tendenziell auch andere technische Wege zur Beibehaltung einer effektiven Werbeblockade beschreiten. Wo allerdings technisch unblockierbare Werbung ausgespielt wird und Zugangssperren oder „Paywalls“ errichtet werden, erreichen die Konterreaktionen tatsächliche und rechtliche Grenzen, die in diesem Abschnitt aufgezeigt werden sollen.

### *1. Darlegung von Konterreaktionen der Werbeblockerbetreiber und Nutzer*

Gewisse technische Reaktionen der Webseitenbetreiber setzen sozusagen einen Schlusspunkt und können nicht gekontert werden. Dies ist der Fall bei generell unblockierbarer Werbung, die durch eine effektive dynamische Generierung von URLs von Filterwerbeblockern schlicht nicht mehr blockiert werden kann. Dies ist ebenso der Fall bei fest mit dem Content verwobener Werbung, die technisch nicht blockierbar ist. Dies mag einer von vielen Gründen sein, warum sich Werbende im modernen Internet gerne den Formen des Native Advertising oder Influencern bedienen<sup>1095</sup>.

Daneben gibt es aber auch Maßnahmen der Webseitenbetreiber, die ihrerseits eine offene Flanke für Gegenangriffe bieten. Bekannte Phänomene werden nachstehend beschrieben. Im Nachgang erfolgt die rechtliche Bewertung der Konterreaktionen.

---

1095 Vgl. obige Beschreibungen unter B. I. 4. b) und d).

## 1. Ergänzung von Werbeblockerfiltern zur Umgehung von Zugangssperren

Unmittelbar nachdem Axel Springer auf Bild.de ihre Zugangssperre installierte, die Nutzern von Werbeblockern den Zugang verweigert, waren in spezialisierten Foren im Web Filterbefehle für Werbeblockersoftware verfügbar, die diese Zugangssperre aushebelten. Diese Umgehung der Zugangssperre führte zu einstweiligen Verfügungsverfahren zwischen Axel Springer und dem AdBlock Plus Betreiber Eyeo GmbH beim LG Hamburg<sup>1096</sup> sowie beim LG und OLG Köln<sup>1097</sup>. Den Verfahren lag laut ihren Tatbeständen der Fall zu Grunde, dass AdBlock Plus im eigenen Forum sowie in dem auf Filterlisten spezialisierten Forum „forums.lanik.us“ zunächst zwei Filterbefehle und später ein „12-zeiliger Code“ zur Einfügung in die Blacklist von AdBlock Plus zur Verfügung stellte. Nach entsprechender Abmahnung waren jedenfalls im eigenen Forum von AdBlock Plus die Filterbefehle noch verfügbar, sodass Axel Springer eine einstweilige Verfügung beantragte und vom LG Hamburg auch erhielt. Eyeo darf dem Beschluss entsprechend weder Programmcodes noch Links zu Programmcodes, noch ganze Filterlisten mit Befehlen verbreiten, die eine Umgehung der Bild.de-Zugangssperre ermöglichen.

Ein ähnliches Vorgehen galt einer Privatperson, die auf YouTube eine Videoanleitung zur Einbindung der Programmcodes zur Umgehung der Zugangssperre auf Bild.de veröffentlicht hat. In einem Hauptsacheverfahren entschied hier das LG Hamburg zu Gunsten von Axel Springer<sup>1098</sup>. Laut Tatbestand des Urteils war folgendes Vorgehen notwendig, um die Bild.de-Sperre mit AdBlock Plus zu umgehen:

- „ – das ABP Icon anklicken und Filtereinstellungen aufrufen,
- die Easylist (+ Easylist Germany) deaktivieren,
- unter [https:// e.a..org/en](https://e.a..org/en) die Liste “ E. without element hiding from“ laden,
- danach entweder die Liste “ Easylist Germany“ hinzufügen (wobei darauf zu achten war, dass man nicht die “ E. + e. Germany“, die man hier findet [https:// e.a..org/en/](https://e.a..org/en/), hinzufügt) oder in ABP als Filterprofil hinzufügen;
- sodann musste man noch eine eigene Liste erstellen
- und sodann diesen Code einfügen mit z.B. STRG+V: @@@|sa-scdn.com^\$domain= b..de @@@|smartadserver.com^\$domain= b..de. “

---

1096 LG Hamburg, Beschluss vom 22.10.2015 und Urteil vom 3.12.2015 – 308 O 375/15, ZUM 2016, 892.

1097 OLG Köln, Beschluss vom 17.12.2015 – 6 W 128/15, (unveröffentlicht).

1098 LG Hamburg, Urteil vom 21.12.2016 – 310 O 129/16, juris.

In der hier maßgeblichen tatsächlichen Betrachtung der Konterreaktion war also die für Adblock Plus notwendige Filterliste um gewisse Sonderbefehle zu ergänzen. Die Programmierung der Sonderbefehle bedurfte wohl besondere Kenntnisse der anwendbaren Programmier- bzw. Auszeichnungssprachen. Sobald diese aber im Internet verbreitet worden sind, war die Einbindung durch den Nutzer leicht zu bewerkstelligen. Deshalb war es auch nicht verwunderlich, dass Axel Springer Rechtsschutz gegen einige prozessual leicht erreichbare Quellen der Verbreitung ersuchten, um die Effektivität der Zugangssperre nicht unmittelbar nach Installation einzubüßen.

## 2. „Adblocker-Detektoren-Blocker“

Neben den oben genannten und für das Verhältnis AdBlock Plus und Bild.de spezifischen Befehlen sind im Netz zudem besondere Add-ons verfügbar, mit denen sich der Ablauf der Adblocker-Detektoren verhindern lässt. Entsprechende Programme sind zum Beispiel Tampermonkey oder Greasemonkey. Dies sind Userscript-Manager Tools, die die Installation von Skripten ermöglicht, die ihrerseits Inhalte von aufgerufenen Webseiten ändern. Konkret ermöglichen sie es dem Benutzer, die Ausführung von JavaScript-Dateien im Browser zu unterbinden, die die angezeigte Webseite mittels DOM-Schnittstelle manipulieren können<sup>1099</sup>. Im Rahmen dieses Add-ons kann dann ein für das spezielle Problem der Adblocker-Detektoren, und folglich auch für Zugangssperren oder Austauschwerbung, ein Skript hinzugefügt werden, etwa der „Anti-Adblock Killer“<sup>1100</sup>. Dieser „Killer“ besteht aus einem JavaScript-Programm und einer speziellen Filterliste, um eine Vielzahl von Webseiten mit Adblock-Detektoren freizuschalten.

## 3. Sonstige Reaktionen

Außerhalb dieser technischen Reaktionen sind auf tatsächlicher Ebene kaum weitere Reaktionen erkennbar. Ein Phänomen, das sich mit dem Erfolg kostenpflichtiger Abo-Modelle wie Netflix und Spotify verbreitet hat,

---

1099 <https://de.wikipedia.org/wiki/Greasemonkey>, zuletzt abgerufen am 31.5.2019.

1100 [https://openuserjs.org/scripts/reek/Anti-Adblock\\_Killer\\_Reek](https://openuserjs.org/scripts/reek/Anti-Adblock_Killer_Reek), zuletzt abgerufen am 31.5.2019.

ist das Teilen von Zugangsdaten zur Überwindung von Bezahlschranken. So ist es nicht selten, dass sich mehrere Personen einen Account bei Netflix oder Spotify teilen, obwohl dies nicht mit den Vertragsbedingungen übereinstimmt – etwa weil diese Bedingungen für die gemeinsame Nutzung vorschreiben, dass alle Nutzer im selben Haushalt leben<sup>1101</sup>. Historisch könnte man dieses Verhalten als eine Art Fortführung der „Piratenkarten“ im Pay-TV Bereich verstehen, wenngleich das Teilen von Zugangsdaten offensichtlich weniger praktischen Aufwand und krimineller Energie bedarf. Dass der Verstoß gegen Vertragsbedingungen negative Rechtsfolgen haben kann, bedarf keiner weiteren Vertiefung. Dasselbe gilt für eine potentielle strafrechtliche Bedeutung des „Passwort-Sharing“.

Eine andere naheliegende Reaktion auf die Wehrreaktionen der Webseitenbetreiber wird allerdings offenbar nicht genutzt: die rechtliche Wehr der Nutzer oder Werbeflockerbetreiber gegen die Anti-Werbeflocker Maßnahmen der Werbeindustrie. Es bleibt abzuwarten, ob im Fortgang der rechtlichen Diskussion eine neue Generation der Werbeflockerfälle auf die Justiz zukommt. Ein gerichtliches Verbot von werbeflockerabhängiger Zwangswerbung würde zum Beispiel eine effektive Konterreaktion darstellen.

## *II. Rechtliche Beurteilung*

Auf Grundlage der zuvor dargestellten Reaktionen soll nachfolgend die rechtliche Zulässigkeit der Umgehung von Zugangssperren und der Umgehung von Zwangswerbung untersucht werden.

### *1. Umgehung von Zugangssperren, § 95a UrhG*

Wie oben bereits beschrieben ist Rechtsprechung verfügbar, die die konkrete Umgehung der Bild.de-Sperre betrifft. Das LG Hamburg hat dabei in zwei Urteilen einen Unterlassungsanspruch aus § 823 Abs. 2 BGB iVm § 95a III Nr. 3 UrhG und § 1004 BGB erkannt<sup>1102</sup>. Rechtlich entscheidend

---

1101 [https://www.chip.de/news/Illegales-Netflix-Streaming-Passwort-Trick-wird-zur-Bedrohung-fuer-den-Streaming-Dienst\\_118683472.html](https://www.chip.de/news/Illegales-Netflix-Streaming-Passwort-Trick-wird-zur-Bedrohung-fuer-den-Streaming-Dienst_118683472.html), zuletzt abgerufen am 31.5.2019.

1102 LG Hamburg, Urteil vom 3.12.2015 – 308 O 375/15, ZUM 2016, 892; Urteil vom 21.12.2016 – 310 O 129/16, juris.

war demnach die Rechtsfrage, ob die Zugangssperre eine wirksame technische Maßnahme gemäß § 95a UrhG ist<sup>1103</sup>. Dies wurde von zwei Kammern des LG Hamburg mit den nachfolgenden darzustellenden Argumenten bejaht, allerdings im Schrifttum angezweifelt. Dieser Abschnitt endet mit einer kurzen Stellungnahme zur Streitfrage.

a) Annahme einer Umgehung einer wirksamen technischen Maßnahme durch das LG Hamburg

Nachdem die 8. Zivilkammer des LG Hamburg bereits am 22.10.2015 mit einem knapp begründeten Beschluss dem Begehren der Betreiber von Bild.de entsprachen und Eyeo per einstweiliger Verfügung untersagte, die Umgehung der Bild.de-Sperre zu fördern, äußerte sich die Kammer in ihrem Urteil vom 3.12.2015 ausführlich zur rechtlichen Beurteilung der Umgehung der Zugangssperre.

Im hier untersuchten Punkt des Vorliegens und der Umgehung einer wirksamen technischen Maßnahme iSv § 95a Abs. 1 UrhG begründete die Kammer ihre Entscheidung wie folgt. Zunächst untersuchte sie die Wirksamkeit der Zugangssperre. Unter Verweis auf die herrschende Rechtsprechung zu dieser Frage prüfte das LG Hamburg, wie schwierig es für einen durchschnittlichen Internetnutzer sei, die hinter der Sperre liegenden Inhalte zu erreichen, wenn er nicht auf den Einsatz von Werbeblockern verzichten wolle. An dieser Stelle könne es jedenfalls nicht auf die Schwierigkeit für einen „Hacker“ ankommen. Es kam zum Ergebnis, dass eine Umgehung für einen Durchschnittsnutzer nicht möglich sei, da hierfür jedenfalls die Fähigkeit gehöre, den JavaScript-Code im Quellcode der Webseite zu verstehen. Mangels einer allgemeinen Verbreitung der Fähigkeit, den Code der für Webseiten geläufigen Auszeichnungs- und Programmiersprachen (HTML, CSS und JavaScript) lesen und verstehen zu können, sei dies also schon ausreichend für das Merkmal der Wirksamkeit. Dies wird dadurch gestützt, dass ergänzend noch die Formulierung von

---

1103 Daneben ging es in den Streitfällen wegen der Veröffentlichung von Umgebungsbefehlen in diversen Foren oder Plattformen um hier nicht darzustellende Zurechnungsfragen. In diesem Zusammenhang lehnte des OLG Köln etwa die Haftung von Eyeo für Einträge in einem fremden Forum („forums.lanik.us“) ab, OLG Köln, Beschluss vom 17.12.2015 – 6 W 128/15, (unveröffentlicht).

Filterbefehlen und die Einfügung dieser in die Blacklist des Werbeblockers notwendig sind.

Weiterer Prüfungspunkt war die Notwendigkeit, dass die technische Maßnahme dem Unterbinden urheberrechtlich relevanter Nutzungshandlungen dienen muss. Dies bejahte die Kammer unter Hinweis auf die Vervielfältigung der auf der Webseite enthaltenen geschützten Lichtbilder und Texte im Arbeitsspeicher des Nutzergeräts. Dies gehe über den urheberrechtlich nicht zu untersagbaren reinen Werkegenuss hinaus. Diskutabel war bei diesem Aspekt ein technisches Detail: Die Sperre wirkt beim erstmaligen Aufruf von Bild.de erst nach einer Dauer von einigen Sekunden. Dies ist die Dauer, in welcher der Adblocker-Detektor seine Arbeit verrichtet und bei erfolgreicher Detektion den Sperrbildschirm einblendet. Man kann also technisch davon sprechen, dass die Vervielfältigung im Arbeitsspeicher bereits abgeschlossen ist und es deshalb tatsächlich nur noch um den reinen Werkgenuss geht. Eine Unterbindung urheberrechtlich relevanter Nutzungshandlungen wäre dann nicht mehr anzunehmen. Außerdem berief sich Eyeo auf § 44a UrhG, also die Schranke für vorübergehende Vervielfältigungen. Dem hielt das LG Hamburg entgegen, dass die konkrete Sperre tatsächlich verhindere, dass im Gerätearbeitsspeicher bereits geladene Elemente in den Browser-Cache verschoben werden. Dies stelle aber eine eigene und neue Vervielfältigung eines Werkes dar, da ein Werk aus dem „unsichtbaren“ Arbeitsspeicher hierdurch erstmals als Bildschirmkopie sichtbar wird<sup>1104</sup>. Eine Anwendung von § 44a UrhG lehnte die Kammer ab, da diese Norm nicht in § 95b UrhG aufgeführt ist und demnach ein systematischer Vorrang der technischen Maßnahme vor der Schrankenregelung bestehe.

Zuletzt bejahte das LG Hamburg eine Umgehungshandlung gemäß § 95a Abs. 3 Nr. 3 UrhG in dem Verbreiten von Softwarecode zur Umgehung. Dies gelte sowohl für die Einfügung in eine Blacklist als auch dem Bewerben solchen Codes in Internetforen.

Ganz ähnlich entschied die 10. Zivilkammer des LG Hamburg in ihrem Urteil vom 21.12.2016<sup>1105</sup>. Sie hielt die mit dem Aufrufen und Anzeigenlassen der Internetseite verbundene Vervielfältigung von geschützten Fotos und Texten für ausreichend, um das Erfordernis von § 95a Abs. 2 UrhG zu erfüllen. Ebenfalls führte es aus, dass § 44a UrhG mangels Nennung in § 95b UrhG nicht anwendbar sei. Die Wirksamkeit der technischen

---

1104 Verweis auf EuGH, Urteil vom 4.10.2011, C-403/08 und C-429/08, GRUR Int 2011, 1063.

1105 LG Hamburg, Urteil vom 21.12.2016 – 310 O 129/16, juris.

Maßnahme begründete die Kammer damit, dass eine Zugangskontrolle stattfinde. Eine Verschlüsselung sei nicht erforderlich. Die Zugangskontrolle anhand der Prüfung der Nutzung eines Werbeblockers sei deshalb wirksam und ausreichend, weil der durchschnittliche Werbeblockernutzer die voreingestellten Filterlisten nicht modifiziere, sondern unverändert lasse. Außerdem könne dieser durchschnittliche Nutzer mangels hinreichender Programmierkenntnisse keinen Code lesen und verstehen. Es mangle Nutzern regelmäßig an der Kenntnis, wie Filterlisten ergänzt werden müssen. Dass diese Kenntnisse durch Recherche im Internet in Spezialforen zugänglich seien, verfange nicht, weil eine solche Recherche nur durch besonders technikaffine Nutzer erfolge, nicht aber durch den durchschnittlichen Nutzer. Zudem ergebe sich aus dem Umstand, dass Umgehungsmöglichkeiten mehr oder weniger ausführlich veröffentlicht worden sind, dass die Schutzmaßnahme nicht für jedermann leicht zu überwinden sei.

b) Kritik in der Literatur

Diese Rechtsprechung fand teils Zustimmung und teils Kritik in der Literatur. Mahnende Worte fand *Peifer* unmittelbar nach der Entscheidung im einstweiligen Verfahren zwischen Axel Springer und Eyeo. Wenngleich er keine ausführliche Prüfung vornahm, äußerte er seine Gedanken zu dieser nächsten Eskalationsstufe im Werbeblockerstreit. Obwohl er die Entscheidung des LG Hamburg als konsequent bezeichnet, weil ein Webseitenbetreiber, der technische Wehrmaßnahmen ergriffen hat, gegen Werbeblocker auch entsprechenden Schutz erhielt, gibt er zu erinnern, dass § 95a UrhG nur dann anwendbar sei, wenn gesetzliche Befugnisse von Rechteinhabern verletzt werden. Die Verbindung von Werbung und Inhalt falle nicht darunter. Aus § 95a UrhG dürfe keine bloße Kopplung von Werbung und Inhalt folgen<sup>1106</sup>. Zudem suggestieren *Nink*<sup>1107</sup> und *Witte*<sup>1108</sup>, dass technische Maßnahmen nach § 95a UrhG vor allem wirksam sein müssen, also nicht einfach und mit geringem Aufwand ausgeschaltet werden können. Während *Nink* sich einem Urteil enthält, lehnt *Witte* die notwendige Wirksamkeit ab, weil Überwindungswerkzeuge im Internet

---

1106 Peifer, AfP 2016, 5, 10; vgl. auch die pseudonyme Kritik unter <https://www.datenschutzbeauftragter-info.de/bildsmart-fragwuerdiges-urteil-des-lg-hamburg-zu-r-adblock-sperre/>, zuletzt abgerufen am 31.5.2019.

1107 Nink, CR 2017, 103, 111.

1108 Witte, ITRB 2018, 34, 38.

leich zu finden seien. Außerdem weist er wie *Peifer* auf eine fehlende Erreichung urheberrechtlicher Schutzziele der Zugangssperre hin. Demnach käme kein Kompletterbot von Umgehungswerkzeugen in Betracht, da damit auch die nicht urheberrechtlich geschützte Gestaltung der Webseite bzw. der Anzeige von nicht geschützten Werbeelementen erfasst würden. § 95a UrhG würde dann durch überschießende Anwendung erlaubtes Verhalten untersagen.

Zustimmend äußert sich hingegen *Runkel* und stellt die Bild.de-Sperre auf dieselbe Stufe mit einer Passwortabfrage bei zugangsgeschützten Webseiten. Außerdem geht er davon aus, dass kostenpflichtige Inhalte, auf die man nur mit Passwort zugreifen kann, mit den werbefinanzierten aber kostenlosen Inhalten gleichzusetzen seien. Wirtschaftlich sei dies vergleichbar und die Werberezeption stelle die Gegenleistung für die Zugänglichmachung der Inhalte dar. Dies mache die Prüfung, ob die Finanzierungsgrundlage im konkreten Fall durch fehlenden Einsatz von Werbeblockern gesichert sei, akzeptabel. Deshalb bestehe kein Grund die Sicherungsmaßnahmen bei Bezahlmodellen anders zu behandeln als die Sicherung des werbefinanzierten Modells<sup>1109</sup>.

Eine ausgesprochen ausführliche Auseinandersetzung – insbesondere in technischer Hinsicht – liefern *Kiersch* und *Kassel*<sup>1110</sup>. In sorgfältiger Prüfung und Subsumtion des § 95a UrhG wird zunächst geprüft, ob eine technische Maßnahme iSv § 95 Abs. 2 S. 1 UrhG vorliegt. In dieser Prüfung differenzieren die Autoren danach, ob durch die jeweilige technische Maßnahme eine Vervielfältigung von geschützten Werken verhindert wird. Dies verneinen sie für die erstmalige Vervielfältigung von Artikeltexten, die bereits mit dem HTML-Dokument in den Arbeitsspeicher der Nutzerrgärts gelangen. Ob weitere Vervielfältigungen im Rahmen des Rendering durch den Browser, z.B. Überföhrung von Texten aus dem Arbeitsspeicher oder Nachladen von Lichtbildern, verhindert werden, hänge von der Programmierung des Adblocker-Detektors und der verbundenen Sperre ab. Ist dieser Zeitpunkt früh genug und verhindere tatsächlich die weitere Arbeit des Browsers am HTML-Dokument so könne durchaus eine ausreichende technische Maßnahme vorliegen, die den Zugriff auf geschützte Werke verhindere. Wirke die Sperre aber erst nach vollständigem Laden und Ausführen, so sei dies zu verneinen. An dieser Stelle widersprechen die Autoren auch behutsam der Ansicht des LG Hamburg, das unter Verweis

---

1109 Runkel, IPRB 2016, 81, 84.

1110 Kiersch/Kassel, CR 2017, 242.

auf die Rechtsprechung des EuGH die Verbringung vom Arbeitsspeicher in Browser-Cache als ausreichende neue Vervielfältigung ansah.

Im sich anschließenden Prüfungspunkt der Wirksamkeit eben jener technischen Maßnahme setzen sich die Autoren mit der Möglichkeit des generellen Verzichts eines Nutzers auf JavaScript durch entsprechende Einstellung im Browser auseinander. Wenn JavaScript-Programme nicht ausgeführt werden, funktioniert demnach auch die Sperre bei Bild.de nicht richtig. Im Ergebnis bekomme der Nutzer Zugriff auf die Webseite, wenn auch unter verringerter Funktionalität, da auch andere JavaScript-Anwendungen nicht ausgeführt werden. Dies führt *Kiersch* und *Kassel* dazu, dass dann praktisch nur die Rezeption der Werke durch die Sperre verhindert werde, nicht aber deren urheberrechtlich relevante Nutzung. Dann bestehe aber auch keine wirksame Schutzmaßnahme. Hingegen wäre eine Sperre in jedem Fall wirksam, wenn sie die Inhalte der Webseite vor Prüfung der Werblockernutzung verschlüsselt oder gar nicht zum Download zulässt. Zwar scheint die Autoren das Argument nicht zu überzeugen, dass der durchschnittliche Internetnutzer selbst praktisch keine eigene Umgehung bewerkstelligen könnte, sie erkennen aber diese Realität an und konstatieren, dass dies ein Grund für die Wirksamkeit darstellen könne.

Bei der Prüfung, ob eine Umgehung im Sinne des § 95a UrhG vorliegt, differenzieren die Autoren wiederum. So soll die Wahl eines Browsers, der generell JavaScript nicht ausführt, oder die Wahl einer Funktion, kein JavaScript auszuführen, jedenfalls nicht zu einer Umgehung führen. Dasselbe gelte beim Einsatz von Scriptblockern wie etwa NoScript. Eine direkte Manipulation der Zugangssperre etwa durch die Greasemonkey und Anti-Adblock-Killer Lösung halten sie dagegen für eine Umgehung. Wenn hingegen keine unmittelbare Ausschaltung der Zugangssperre vorliegt, sondern vielmehr dem dazu gehörigen Adblocker-Detektor technisch vorgegaukelt wird, dass das Köderelement vom Nutzergerät geladen und angezeigt wird, möge zu unterscheiden sein, ob die Fallgestaltung auf einer Ausschaltung von JavaScript generell beruht oder eine gewollte Umgehung darstellt. Im ersten Fall müsse zur Wahrung der Konsistenz mit der ersten dargestellten Fallgruppe eine Umgehung ausscheiden, im zweiten Fall läge hingegen eine Umgehung vor.

Im Ergebnis versuchen *Kiersch* und *Kassel* den Ausgleich zwischen der Freiheit der Nutzer, JavaScript-Anwendungen zu meiden, und den direkten Umgehungsversuchen bei Bild.de zu finden. Die vorgenommene differenzierende Betrachtung steckt dafür einen sinnvollen Rahmen.

c) Stellungnahme

Auf dieser Grundlage soll nachfolgend Stellung genommen werden, wobei nicht allein auf die Bild.de-Sperre einzugehen ist, sondern das Thema Umgehung von Zugangssperren auf Webseiten abstrakt betrachtet werden soll. Dazu bedarf es einer genauen Beachtung der rechtlichen Anforderungen und der technischen Gegebenheiten. Eine rein wirtschaftliche Betrachtung wie *Runkel* sie vornimmt, wird der Komplexität in jedem Falle nicht gerecht. Auch die von *Peifer* und *Witte* geäußerten Zweifel vor dem Hintergrund des Schutzzwecks scheinen zu pauschal. *Kiersch* und *Kassel* bereiten das Thema sorgsam auf, jedoch ist ihren Ergebnissen nicht in allen Punkten zuzustimmen.

§ 95a Abs. 1 UrhG enthält ein Umgehungsverbot für wirksame technische Maßnahmen zum Schutz eines nach dem UrhG geschützten Werkes oder Schutzgegenstandes. § 95a Abs. 2 UrhG enthält die anwendbaren Definitionen für die technische Maßnahme und für deren Wirksamkeit. Sowohl im Text des Umgehungsverbots als auch bei den Definitionen ist der Schutz von Werken oder sonstigen Schutzgegenständen des UrhG ausdrücklich genannt. Dies zeigt deutlich, dass es unbedingte Grundlage der Anwendung von § 95a UrhG ist, dass die Zugangssperre auf die Verhinderung von urheberrechtlich relevanten Nutzungshandlungen abzielt. Wie oben ausführlich herausgearbeitet, ist der Besuch einer Webseite insgesamt nicht urheberrechtlich relevant<sup>1111</sup>. Deshalb kann eine Zugangssperre nicht schon deshalb den Schutz von § 95a UrhG auslösen, weil sie die bloße Rezeption von Webseiten – mit oder ohne Werbung – verhindern soll. Richtigerweise stellt das LG Hamburg deshalb auf den gleichwohl existierenden urheberrechtlichen Schutz von einzelnen Elementen einer Webseite ab. Journalistische Texte, Fotos und Videos sind für sich gesehen selbstredend schutzfähige Werke oder zumindest durch Leistungsschutzrechte erfasste Gegenstände.

Allerdings ergibt sich hier eine gewisse Diskrepanz zwischen dem Ziel der Zugangssperre und den eigentlich von § 95a UrhG geschützten Werken und Schutzgegenständen. Bei oberflächlicher Betrachtung geht es nämlich nicht um einen Schutz vor Raubkopien von journalistischen Texten, Fotos oder Videos, auf den § 95a UrhG eigentlich zugeschnitten ist. Vielmehr versuchen Webseitenbetreiber durch die Einführung von Selbsthilfemaßnahmen einen überschießenden Schutz zu erreichen, was

---

1111 Siehe oben Ziffer C. I. 4. a) bb).

ein durchaus kritisiertes Problem bei der Anwendung der Norm ist<sup>1112</sup>. Gleichwohl führt an diesem überschießenden Schutz wohl kein Weg vorbei. Nur wenn die Umgehungslösung tatsächlich teilbar ist, kann ein Gericht lediglich ein Teilverbot aussprechen, etwa wenn ein Werbeblocker nur eine gewisse abgrenzbare Funktion aufwiese, die die Umgehung bewerkstelligt. In Fallkonstellationen wie sie dem LG Hamburg vorlagen kommt nur ein Kompletต์verbot der Umgehung in Betracht.

Wenn nicht über das Merkmal des Werks oder Schutzgegenstands differenziert werden kann, muss die urheberrechtliche Nutzungshandlung untersucht werden. Da bei der Nutzung von Webseiten (bzw. deren Elementen) die Vervielfältigung maßgeblich ist, muss untersucht werden, ob eine Vervielfältigung der maßgeblichen Texte und Fotos durch die Zugangssperre verhindert wird. Dies kann ganz unterschiedlich ausgestaltet sein. Die Parteien im Streitfall des LG Hamburg im Verfahren 308 O 375/15 stritten auf Grundlage von Sachverständigengutachten zur technischen Wirkung, ob die Vervielfältigung der Werke bereits unterbunden wird, bevor die Elemente der Internetseite vollständig in den Speicher des Betriebssystems des Nutzers kopiert werden oder erst dann, wenn die Elemente vom Speicher des Betriebssystems in einen anderen Teil des Arbeitsspeichers, den Browser-Cache, verschoben werden<sup>1113</sup>. Bei anderen Webseiten ist beim Besuch ganz deutlich, dass die gesamte Startseite einer Webseite vollständig geladen und auf dem Gerät bereits angezeigt wird, bevor die Zugangssperre zu wirken beginnt und auf einen Sperrbildschirm weiterleitet. Demnach hängt die Beurteilung der Rechtswidrigkeit einer Umgehung grundsätzlich davon ab, ob die Zugangssperre eine Vervielfältigung verhindert oder lediglich nach bereits erfolgter Vervielfältigung den „Werkgenuss“ vermeidet. Im ersten Fall ist rechtlich, technisch und wertungsmäßig der Schutz des Webseitenbetreibers geboten. Der zweite Fall genügt hingegen auf den ersten Blick nicht den rechtlichen Anforderungen, weil keine von § 95a Abs. 2 UrhG geforderte Technologie vorliegt, die im normalen Betrieb dazu bestimmt ist, Werke oder Schutzgegenstände betreffende ungenehmigt Handlungen zu verhindern oder einzuschränken. Praktisch sind solche Technologien, die jede Vervielfältigung zunächst unterbinden, bis die Adblockernutzung geklärt wurde, durchaus möglich. Deshalb könnte auf den ersten Blick ein Webseitenbetreiber, der eine solche technisch unvollkommene Sperre einsetzt auch nicht schutzbedürftig sein.

---

1112 Vgl. Wandtke/Ohst, in: Wandtke/Bullinger, UrhG, § 95a, Rn. 3.

1113 ZUM 2016, 892, 897.

Allerdings werden durch die nach Laden einer Startseite der Landing Page nachträglich einsetzende Sperre weitere Vervielfältigungshandlungen unterbunden. Beim normalem Browsen durch das Internet werden nicht nur Startseite, sondern auch darauf verlinkte Unterseiten, z.B. die ausführlichen Beiträge einer Nachrichtenseite, besucht. Wenn man nun aus dem schlichten Umstand, dass die Startseite bereits einmal im Arbeitsspeicher vervielfältigt worden ist, die gesamte Umgehung einer Zugangssperre erlauben würde, könnte der Nutzer auch auf alle Unterseiten zugreifen. Und deren erstmalige Vervielfältigung wird durch die Zugangssperre zweifelsohne wirksam unterbunden, weil der Nutzer durch den Sperrbildschirm daran gehindert wird, weiter auf der Webseite zu browsen. Bei einer Gesamtbetrachtung der Nutzung von Webseiten kommt es deshalb wohl gar nicht – wie beim LG Hamburg im Verfahren 308 O 375/15 behandelt – darauf an, ob man zwischen Cachekopien und Bildschirmskopien unterscheidet. Der Schwerpunkt der Zugangssperre liegt auf der Verhinderung der Erreichung anderer Seiten als der Startseite. Hierin sind weitere wertvolle Werke und Schutzgegenstände der Contentanbieter enthalten. Ein vollständiger Zugriff des Nutzers auf die Webseite nach Umgehung einer Zugangssperre ist deshalb grob unbillig und nicht gerechtfertigt.

Im Übrigen ist dem Nutzer mit einer auf Startseiten begrenzten zulässigen Umgehung nicht geholfen, weil die Umgehungsmaßnahmen nicht differenzieren. Entweder die Zugangssperre wird mit Wirkung für alle Seiten umgangen oder eben gar nicht. Wenn dem umgehenden Nutzer ein Artikel auf der „zu Recht“ freigeschalteten Startseite gut gefällt, würde er bei fortgesetzter Umgehung der Zugangssperre zu den noch nicht vervielfältigten Texten, Fotos und/oder Videos der Unterseite gelangen und somit gegen § 95a UrhG verstoßen. Deshalb wird man wohl generell Umgehungsmaßnahmen im Web an § 95a UrhG messen müssen. Eine partielle Zulässigkeit der Umgehung für Startseiten und Deep-Links ist praktisch nicht umzusetzen.

Als Zwischenergebnis ist demnach festzuhalten, dass durch Zugangssperren auf Webseiten urheberrechtlich relevante Vervielfältigungshandlungen verhindert werden, spätestens auf Unterseiten. Sie sind demnach als technische Maßnahmen gemäß § 95a Abs. 2 S. 1 UrhG anzusehen, die grundsätzlich dem Umgehungsschutz zugänglich sind.

Ergänzend muss aber noch die Wirksamkeit der technischen Maßnahme nach § 95a Abs. 2 S. 2 UrhG gegeben sein, damit eine Umgehung verboten ist. Dies ist der Fall, wenn die oben identifizierten Vervielfältigungen durch „eine Zugangskontrolle, einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung oder einen Mechanismus zur Kontrolle

der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten“ werden. Ob die Zugangssperre nun als Zugangskontrolle oder Schutzmechanismus einzuordnen ist, ist nicht entscheidend. Dies ist vielmehr das Merkmal des „Unter-Kontrolle-Haltens“ von Vervielfältigungen im Nutzergerät. Zu Recht geht das LG Hamburg davon aus, dass Wirksamkeit nicht bedeutet, dass jegliche Umgehungsmöglichkeit tatsächlich ausgeschlossen ist. Das Schutzniveau muss vielmehr gegenüber dem Kreis der potentiellen Angreifer ausreichend hoch angesetzt worden sein, wobei auch mit Recht vom durchschnittlichen Internetnutzer und nicht von Hackern oder besonders technikaffinen Nutzern ausgegangen werden darf<sup>1114</sup>.

Setzt man diesen Maßstab an, ist auch absolut richtig, dass der Großteil der Internetnutzer keinen Schimmer von der Gestaltung des Codes von Webseiten hat und somit selbst keine Umgehung programmieren kann. Der Umstand, dass im Internet Umgehungshilfen angeboten werden, bestärkt insoweit, dass die Zugangssperre nicht einfach umgangen werden könne, so das LG Hamburg<sup>1115</sup>. Aber kommt es wirklich darauf an, dass ein Nutzer selbst und eigenverantwortlich die Sperre umgeht? Oder reicht es nicht aus, dass der Nutzer im Internet von entsprechend befähigten Programmierern die Anleitung erhalten kann, um die Sperre zu umgehen? Mit anderen Worten: wenn es praktisch nicht schwierig ist, eine Anleitung mit vorformulierten Codes oder Anwendungen zu finden und anzuwenden, ist die Sperre dann wirksam? Dabei gilt zu beachten, dass die Verwehrung solcher externen Hilfe zu einer Diskrepanz zwischen der Stufe des Werbeblockens und der Stufe der Erwehrung gegen Zugangssperren führen könnte. Auf der ersten Stufe kann nämlich nicht geleugnet werden, dass kaum ein Nutzer ohne Einbindung der entsprechenden Software und Filterbefehle effektiv Werbung blocken könnte. Genauso nimmt der durchschnittliche Nutzer, wenn er sich durch Zugangssperren gestört fühlt, verfügbare Hilfe in Anspruch. Dies umso mehr, wenn diese Hilfe durch für jedermann mögliche Schritte wie eine Google-Suche verfügbar ist.

Der BGH führte in *Werbeblocker II* aus, dass die Inanspruchnahme von technischer Hilfe auch dann nicht unzulässig ist, wenn sie zu einem Ergebnis führt, dass der Nutzer nicht alleine hätte bewirken können<sup>1116</sup>. Wenn die Nutzung von Hilfe bei der Werbeblockade demnach erlaubt

1114 LG Hamburg, Urteil vom 21.12.2016 – 310 O 129/16, juris.

1115 LG Hamburg, Urteil vom 21.12.2016 – 310 O 129/16, juris.

1116 BGH, Urteil vom 19.4.2018 – I ZR 154/16, WRP 2018, 1322 – *Werbeblocker II*.

ist, kann man durchaus hinterfragen, ob dies bei der Ausschaltung der Zugangssperre wirklich die Wirksamkeit der technischen Maßnahme begründen kann. Doch lässt sich das im Rahmen von § 4 Nr. 4 UWG geäußerte Argument des BGH in *Werbeblocker II* wohl nicht auf die Interessenlage von § 95a UrhG übertragen. Die Werbung im Internet ist ein isoliertes Element innerhalb einer nicht schutzfähigen Webseite und nicht etwa eine technische Maßnahme iSv § 95a Abs. 2 S. 1 UrhG. Deshalb ist die Blockade dieser Elemente etwas vollkommen anderes als die Umgehung der Zugangssperre. Also liegt tatsächlich kein unmittelbarer Widerspruch vor. Der Gedanke des BGH kann aber insoweit Geltung erlangen, dass er bei der Bestimmung der von den durchschnittlichen Internetnutzern zu erwartenden Anstrengungen zur Umgehung einer solchen Zugangssperre herangezogen wird. Insoweit sind einfache Lösungen, wie die Installation eines Browser-Add-ons, durchaus realistischerweise von Nutzern zu erwarten, die eine Zugangssperre unwirksam machen wollen. Es kommt gerade nicht darauf an, ob ein Nutzer Programmierkenntnisse hat und eine Umgehungslösung selbst programmieren kann. Entscheidend ist, ob er sich mit einfachsten Mitteln behelfen kann. Dies kann bei einer Verbreitung von Umgehungsanleitungen im Web bejaht werden.

Auf einem anderen Blatt steht, ob diese Hilfe für einen Nutzer im Einzelfall leicht auffindbar und umsetzbar ist. Dies kann bei der oben beschriebenen Anti-Adblock-Killer Lösung durchaus verneint werden, weil hier zunächst eine neue Software wie Greasemonkey geladen werden muss, in welchem dann wiederum das Tool Anti-Adblock-Killer integriert werden muss. Zwar ist die Information über diese Umgehungslösung durch eine Google-Suche relativ leicht zu finden, für den durchschnittlichen Nutzer könnte diese jedoch (noch) zu kompliziert sein. Hierauf zielen die Ausführungen der 10. Kammer des LG Hamburg ab, die unter anderem ausdrücklich darauf hinweisen, dass der durchschnittliche Nutzer nicht wisse, wie man JavaScript im Browser deaktiviere. Dies hat die Kammer aus eigener Kenntnis beurteilt, weil sie sich zu den durchschnittlichen Nutzern gezählt haben<sup>1117</sup>. Jedoch ist zu beachten, dass mit dem Fortschritt von „digital literacy“ in der Gesellschaft, d.h. der Zunahme von Kenntnissen über Vorgänge und Möglichkeiten im digitalen Bereich, auf lange Sicht nicht mehr vom „ahnungslosen“ Internetnutzer ausgegangen werden kann. Der Maßstab des durchschnittlichen Internetnutzers ist nach hier vertretener Ansicht im Fluss vom „flüchtigen“ hin zum „verständigen“ Internetnutzer. Diesem dürften dann auch nicht allzu schwere Aktio-

---

1117 LG Hamburg, Urteil vom 21.12.2016 – 310 O 129/16, juris.

nen wie die Änderungen von Browsereinstellungen zur Deaktivierung von JavaScript zugetraut werden.

Die Wirksamkeit der Zugangssperren auf Webseiten wird man also in jedem Einzelfall neu bewerten müssen. Dass das LG Hamburg die Bild.de-Sperre als wirksam angesehen hat, ist dabei vor dem Hintergrund der konkret behandelten eher komplizierten Anpassung der Filterliste innerhalb von Adblock Plus verständlich und verdient Zustimmung. Dies kann aber sicherlich nicht als allgemeine Regel für jede Art von Umgehungsmaßnahme gegen jede Zugangssperre gelten. Auch hier ist das weitere Wettrüsten der verfeindeten Lager abzuwarten<sup>1118</sup>.

Die Ausschaltung eines Vorgangs, der das Vorhandensein von Werbeblockern beim Nutzer prüft, ist auch eine Umgehung im Sinne von § 95a Abs. 1 UrhG. Der Begriff der Umgehung ist sehr weit und erfasst alle Handlungen, die zu einer Verwertung im Sinne des Urheberrechts führen<sup>1119</sup>. Dieses Merkmal haben *Kiersch* und *Kassel* in ihrem Beitrag weitgehend überzeugend geprüft<sup>1120</sup>. Insbesondere ist die verbreitete „Anti-Adblock-Killer“-Lösung eine klare Umgehung. Wird die Zugangssperre hingegen nur beiläufig von Scriptblockern, durch Ausschaltung von JavaScript im Browser oder die Wahl rein textbasierter Browser ausgehebelt, ist dies keine Umgehung, sondern eine Schwäche der Schutzmaßnahme. Interessant ist die Frage, ob eine Maßnahme, die dem Adblocker-Detektor „vorgaukelt“ den Köder geschluckt zu haben, eine Umgehung darstellt. Nach der zuvor genannten abstrakten Definition, wonach allerlei Manipulationsvorgänge zu fassen sind, wenn damit eine Vervielfältigung eigentlich geschützter Werke verbunden ist, muss auch diese Art der Umgehung erfasst sein. Eine zweckmäßige Abgrenzung erfolgt dann über das Merkmal der Wirksamkeit. Wenn ein Webseitenbetreiber nur einen einzigen Köder legt, der auch leicht zu identifizieren ist, sollte keine Wirksame technische Maßnahme vorliegen. Wenn hingegen eine ausgeklügelte technische Maßnahme mit mehreren Köderelementen genutzt wird, sollte von einer wirksamen Maßnahme ausgegangen werden, die durch eine Manipulation umgangen wird.

Insgesamt ist die Umgehung einer Zugangssperre zu einer Webseite also in den folgenden Fällen unter § 95a UrhG zu subsumieren und verboten:

- Wenn die Umgehung profunde Programmierkenntnisse benötigt und die Umgehungslösung nicht leicht im Internet auffindbar und/oder

1118 Vgl. zum Gedanken des Wettrüstens etwa Witte, ITRB 2018, 34, 39.

1119 Wandtke/Ohst, in: Wandtke/Bullinger, UrhG, § 95a, Rn. 53.

1120 Kiersch/Kassel, CR 2017, 242.

leicht im Nutzergerät umsetzbar sind. Hierunter lassen sich die Bild.de-Fälle vor dem LG Hamburg subsumieren.

- Wenn die Umgehung wie beim „Anti-Adblock-Killer“ die Installation mehrerer Add-ons benötigt und die Lösung unmittelbar dazu dient, die Zugangssperre zu umgehen und Inhalte ohne Werbung zu genießen, die im Normalfall der Internetnutzung nicht ohne Werbung zur Verfügung stehen.
- Wenn die Umgehung auf einer Manipulation der Adblocker-Detektion beruht, die vorgaukelt, dass eine ausgeklügelte und quantitativ und/oder qualitativ komplexe Köderlogik im Nutzergerät angezeigt wird.

Keine verbotene Umgehung liegt hingegen vor, wenn

- Die Umgehungslösung für jeden Nutzer, der in der Lage ist einen Werbeblocker zu installieren, derart leicht im Internet zu finden und im eigenen Gerät umzusetzen ist, dass die Zugangssperre als unwirksam zu bewerten ist. Dies wäre etwa der Fall, wenn ein Nutzer durch eine einfache Google-Suche eine brauchbare Umgehungslösung findet, die nur wenige Klicks zur effektiven Implementierung im Nutzergerät benötigt.
- Wenn die Nutzung von Skriptblockern oder die Auswahl einer Browser-einstellung dazu führt, dass die Zugangssperre (oder ein Teil davon) nicht ausgeführt wird. Allerdings muss hier einschränkend gelten, dass eine differenzierende Wirkung solcher Anwendungen und Einstellungen nicht akzeptabel ist, wenn sie alle für den Nutzer „vorteilhaften“ JavaScript-Anwendungen zulässt und nur unliebsame JavaScript-Anwendungen blockiert (sozusagen ein JavaScript-Whitelisting).
- Wenn die Umgehung auf einer Manipulation der Adblocker-Detektion beruht, die vorgaukelt, dass technisch banale Köder im Nutzergerät angezeigt werden.

## 2. Umgehung von Zwangswerbung

Keine Rechtsprechung existiert dagegen für die Umgehung von Lösungen, die den Nutzern Zwangswerbung ausspielen. Deshalb soll an dieser Stelle geprüft werden, inwiefern die obigen Gedanken übertragbar sind. Außerdem soll bewertet werden, ob eine Anwendung wie „Anti-Adblock Killer“ eine zulässige Reaktion auf Zwangswerbung ist.

Diese Bewertung hängt ebenso wie die Prüfung der Zugangssperren davon ab, ob die Zwangswerbung als wirksame technische Maßnahme gemäß § 95a UrhG bewerten werden kann. Dies ist nach den vorgehenden

abstrakten Beschreibungen jedoch schnell beantwortet: Zwangswerbung fällt nicht unter § 95a UrhG. Dies liegt daran, dass hier keine Vervielfältigung von urheberrechtlich geschützten Werken und nach dem UrhG geschützten Gegenständen verhindert wird. Der Zugang zur Seite und ihren Inhalten bleibt ja gerade möglich. Die Verknüpfung von Werbung und Content hingegen ist nicht urheberrechtlich geschützt. Deshalb liegt ohne Zweifel keine technische Maßnahme iSv § 95a Abs. 2 S. 1 UrhG vor.

Da oben bereits festgestellt worden ist, dass die Zwangswerbung eine unzumutbare Belästigung der Nutzer darstellt<sup>1121</sup> ist eine solche Reaktion von Webseitenbetreibern auch nicht aus anderen Gründen schutzwürdig. Die Ausspielung von Zwangswerbung darf von Nutzern demnach allein schon aus Gründen des Selbstschutzes vor einer verbotenen Handlung umgangen werden.

Dies führt allerdings zur brisanten Frage, wie Nutzer diese Umgehung bewerkstelligen können. Während generell unblockierbare Werbung – wie die Beschreibung schon deutlich macht – nicht durch Werbeblockertechnologien zu verhindern sind, bleibt hier wohl nur die rechtliche Wehr. Anders bei der Austauschwerbung nach erkannter Werbeblockernutzung. Hier kann die Wirkung des Adblocker-Detektors umgangen werden. Wie im Zusammenhang mit Zugangssperren schon beschrieben kann dem Detektor vorgegaukelt werden, dass die ausgelegten Köder im Nutzergerät geladen worden sind. Daneben würden findige Programmierer nach Studium der Wirkweise konkreter Austauschwerblösungen sicher weitere Umgehungen entwickeln können.

Eine weitere Lösung ist der bereits mehrfach genannte „Anti-Adblock Killer“. Dieser führt zu einer Verhinderung JavaScript-basierter Adblocker-Detektoren. Bei Zwangswerbung in Form der Austauschwerbung ist diese Lösung ein probates Mittel zur Ausschaltung. Allerdings wurde im Zusammenhang mit Zugangssperren das Ergebnis gefunden, dass diese Lösung eine nicht zulässige Umgehung nach § 95a UrhG darstellt. Für einen legalen Einsatz dieser Lösung müsste also sichergestellt sein, dass der „Anti-Adblock Killer“ nur die Seiten mit Zwangswerbung tangiert, nicht aber die den Webseitenbetreibern vorbehaltenen Zugangssperren. Dies könnte theoretisch über Whitelists umgesetzt werden. Auf dieser differenzierenden Basis wäre der Einsatz dieser Lösung demnach zulässig. Es bleibt abzuwarten, ob hier in Zukunft ggf. konkrete Hilfemaßnahmen für

---

1121 Siehe oben Ziffer E. II. 2. a).

Nutzer angeboten werden, die die Austauschwerbung verhindern. Rechtlich sind diese jedenfalls zu billigen<sup>1122</sup>.

---

1122 Gegen den Vorwurf einer gezielten Behinderung von Webseitenbetreibern oder Anbietern von Zwangswerbungslösungen wie „AdDefend“ lässt sich vorbringen, dass diese sich selbst nicht im wettbewerbsrechtlich rechtmäßigen Rahmen bewegen. Eine Reaktion auf diese rechtmäßige Handlung wäre dann wohl im Rahmen einer Interessenabwägung als zulässig zu erachten.