

Luther.

Newsletter IP/IT

4. Ausgabe 2018

Inhalt

Datenschutzkonferenz: Cookies und Tracking nur noch mit Einwilligung | [Seite 3](#)

Know-How-Richtlinie: Neue Vorgaben für den Knowhow- und Geheimnisschutz | [Seite 5](#)

BGH: Bonusaktion für Smartphone-App „My Taxi“ | [Seite 8](#)

BGH: Bei offensichtlichen (Urheber-) Rechtsverletzungen sind Internet-Provider zur Speicherung von Daten verpflichtet | [Seite 9](#)

Veranstaltungen und Veröffentlichungen | [Seite 11](#)

Datenschutzkonferenz: Cookies und Tracking nur noch mit Einwilligung

Seit Ende April verunsichert eine Stellungnahme der Datenschutzkonferenz Webseitenbetreiber und Marketingagenturen. Die Datenschutzkonferenz (DSK) als Zusammenschluss der unabhängigen Datenschutzbehörden des Bundes und der Länder hat eine aktuelle Positionsbestimmung veröffentlicht, in der sie zu den Voraussetzungen von Analyse- und Trackingtools Stellung bezogen hat: Danach dürfen Tools wie Google Analytics, eTracker und Matomo (vormals: Piwik) nur noch eingesetzt werden, wenn der Besucher der Webseite vorab in das Tracking und die Analyse seines Nutzerverhaltens ausdrücklich eingewilligt hat.

Hintergrund: DSGVO vs. TMG

Am 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Als EU-Verordnung ist sie unmittelbar geltendes Recht in Deutschland. Die Regelungen der DSGVO treten in Konkurrenz zu anderen deutschen Gesetzen. Der deutsche Gesetzgeber hat es nämlich versäumt, eine Reihe von nationalen Gesetzen an die DSGVO anzupassen.

Eine dieser Normen ist § 15 Abs. 3 Telemediengesetz (TMG). Diese Vorschrift regelte bislang, unter welchen Voraussetzungen der Einsatz von Tracking- und Analysetools zulässig war. Insbesondere mussten etwaige personenbezogene Daten, z.B. die IP-Adresse, als Pseudonyme verarbeitet werden. Zudem musste der Webseitenbesucher in der Datenschutzerklärung darüber informiert werden, dass solche Tools eingesetzt werden und wie er dem Einsatz widersprechen konnte. In der Vergangenheit hatten sich hierzu Standardtexte und Maßnahmen etabliert. Google und die zuständige Datenschutzaufsichtsbehörde hatten sich sogar darüber abgestimmt, unter welchen Voraussetzungen Google Analytics datenschutzkonform eingesetzt werden durfte.

Durch die DSGVO wird die Regelung des § 15 Abs. 3 TMG verdrängt, da die DSGVO als europäisches Primärrecht „Anwendungsvorrang“ genießt, also vorrangig vor den nationalen Regelungen anzuwenden ist. In der DSGVO fehlt jedoch eine Regelung, die mit § 15 Abs. 3 TMG vergleichbar wäre. Weil es sich bei dem Tracking (wohl) um die Verarbeitung von personenbezogenen Daten handelt, ist dies nur zulässig, wenn die DSGVO hierfür eine entsprechende Erlaubnis vorsieht.

Die Entscheidung

Nach Ansicht der Datenschutzkonferenz bedarf es beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen sowie bei einer Erstellung von Nutzerprofilen, einer vorherigen ausdrücklichen Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO. Notwendig ist also eine ausdrückliche Zustimmung zum Einsatz dieser Technologien. Dies betrifft auch gängige Tracking Tools wie Google Analytics und Matomo (ehemals Piwik). Bei deren Einsatz muss jetzt eine informierte Einwilligung eingeholt werden, bevor überhaupt Cookies gesetzt oder ausgelesen werden. Dies ist technisch durch eine Cookie-Wall möglich: Beim ersten Besuch der Webseite erscheint ein „Overlay“, in dem die Einwilligung zum Einsatz von Cookies eingeholt wird. Auch nach Ansicht der Datenschutzkonferenz gilt das Einwilligungserfordernis nicht für Cookies, die der technischen Bereitstellung der Website dienen, also etwa solche, die für den Warenkorb eines Online-Shops eingesetzt werden. Bloße Hinweisbanner auf das Platzieren von Cookies gelten jedoch nicht als Einwilligung.

Kritik an dem Beschluss

Die Darstellung der Datenschutzkonferenz ist in weiten Teilen zutreffend, insbesondere wenn es um den Vorrang der DSGVO vor dem TMG geht. Problematisch ist aber die Schlussfolgerung der Datenschutzkonferenz, dass ein Tracking nur mit vorheriger Einwilligung zulässig sei. Erstaunlich ist vor allem, dass sie derart pauschal und ohne weitere Begründung erfolgt ist. Denn grundsätzlich ist das Tracking und das Anlegen von Nutzerprofilen nicht nur allein auf Basis einer Einwilligung möglich. Eine



Rechtfertigung dieser Maßnahmen kann nämlich ebenso auf der Basis der berechtigten Unternehmensinteressen nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO erfolgen. Dafür bedarf es einer Interessenabwägung. Anhaltspunkte, dass hier stets die Interessen der Nutzer überwiegen, sind jedenfalls in der DSGVO nicht zu erkennen. Vielmehr gibt die DSGVO bereits innerhalb der Erwägungsgründe Hilfestellungen an die Hand, die bei der Interessenabwägung herangezogen werden können. So ist dort etwa festgehalten, dass Direktwerbung als ein berechtigtes Interesse des Unternehmen betrachtet werden kann. Damit dürfte das Tracking, als grundsätzlich weniger eingriffsintensive Maßnahme, ebenfalls vom berechtigten Interesse gedeckt sein. Hierfür spricht auch Art. 21 Abs. 2 DSGVO, der für Fälle des Profilings im Rahmen der Direktwerbung ein Widerspruchsrecht einräumt. Dies wäre nicht notwendig, wenn ein solches Profiling ausschließlich auf Grundlage einer Einwilligung zulässig wäre, denn dann bestände ohnehin kein Widerspruchsrecht. Die Entscheidung der Datenschutzkonferenz ist somit keine zwangsläufige Folge der DSGVO.

Unser Kommentar

Das Positionspapier ist zunächst nur die Meinung der Datenschutzbehörden zum Einsatz dieser Tools. Diese Verlautbarung ist weder ein Gesetz noch bindet sie die Gerichte bei ihrer Entscheidung. Allerdings hat die Meinung der Datenschutzaufsichtsbehörden einiges Gewicht. Damit dürfte die Ansicht weitreichende Folgen für die Praxis nach sich ziehen.

Die Stellungnahme der Aufsichtsbehörden hat, ob nun bewusst oder unbewusst, unmittelbare Auswirkungen auf die wettbewerbsrechtliche Praxis. Es gab bereits erste Abmahnungen von sogenannten Abmahnanwälten, welche mangelnde Einwilligungen als Verstöße gegen die datenschutzrechtlichen Bestimmungen kostenpflichtig geltend gemacht haben. Hier kommt die Ansicht der Behörden als Argumentationsgrundlage gerade rechtzeitig.

Für Webseitenbetreiber stellt sich damit die Frage, wie sie sich verhalten sollen. Zunächst können diese Anbieter auf den Einsatz derartiger Tools verzichten, bis die Rechtslage geklärt ist. Sie können auch weiterhin die Tools einsetzen und im Fall einer Abmahnung oder einer Beanstandung durch die Datenschutzaufsichtsbehörden ein Gerichtsverfahren anstrengen. Damit trägt man aber das Risiko, dass sich das Gericht nicht der Ansicht der Datenschutzkonferenz anschließt. Schließlich können Webseitenanbieter auch eine Cookie-Wall installieren und die notwendige Einwilligung einholen. Dann müssen sie kurzfristig die notwendigen technischen Anpassungen vornehmen. Damit geht das Risiko einher, dass die Entscheidung der Datenschutzkonferenz zukünftig revidiert wird und die Aussagen der Analysen verfälscht werden, weil nicht mehr von jedem Besucher die entsprechenden Daten zur Verfügung stehen.

Know-How-Richtlinie: Neue Vorgaben für den Know-how- und Geheimnisschutz

Ab 9. Juni 2018 gelten die neuen europäischen Vorgaben für den Geheimnisschutz, denn dies ist das Ablaufdatum der im Rahmen der sog. „Know-How Richtlinie“ vorgegebenen Frist für die Umsetzung in nationales Recht. Daneben gibt es einen aktuellen Referentenentwurf zur Umsetzung der Know-How Richtlinie in ein deutsches „Gesetz zum Schutz von Geschäftsgeheimnissen“ (offizielle Abkürzung: GeschGehG).

Hintergrund

Geschützt wird Know-how in Deutschland derzeit als Betriebs- bzw. Geschäftsgeheimnisse über das Wettbewerbsrecht (Geheimnisschutz). Dabei handelt es sich bei den wettbewerbsrechtlichen Vorschriften (§ 17 UWG) um Strafvorschriften, die den unberechtigten Abfluss von Know-how unter Strafe stellen. Eine zivilrechtliche Zuordnung dieses Know-hows zu einem bestimmten Unternehmen als Inhaber, vergleichbar mit den gewerblichen Schutzrechten, wie Patent- oder Markenrechte, findet über den Geheimnisschutz jedoch nicht statt, sondern wird vielmehr vorausgesetzt.

Aufgrund der zunehmenden digitalen und grenzüberschreitenden Zusammenarbeit zwischen Unternehmen und der enormen wirtschaftlichen Bedeutung betrieblichen Know-hows hat sich die Europäische Union dazu entschieden, einen einheitlichen europäischen Geheimnisschutz zu schaffen. Mit der Know-how-Richtlinie, die bis Juni 2018 in nationales Recht umgesetzt werden muss, kommt es zu weitreichenden Veränderungen, die Unternehmen bereits jetzt zu einem Handeln zwingen, wenn sie auch künftig ihr betriebliches Know-how geschützt wissen wollen.

Das „Geschäftsgeheimnis“ – Was ist geschützt?

Der Anwendungsbereich des GeschGehG ist eröffnet, wenn ein „Geschäftsgeheimnis“ im Sinne des § 1 Nr. 1 vorliegt. Nach der Entwurfsbegründung soll diese Definition – im Zusammenspiel mit den kumulativ zu erfüllenden qualitativen Voraussetzungen Unbekanntheit, Wert, Maßnahmen – sowohl die bisher gebräuchlichen Begriffe des „Know-Hows“ als auch des im deutschen Raum üblichen „Betriebsgeheimnisses“ umfassen. Bei solchen Informationen kann es sich also sowohl um technisches wie auch um kaufmännisches Wissen handeln.

In der qualitativen Voraussetzung der „Schutzmaßnahmen“ liegt eine der zentralen Neuerungen des Geheimnisschutzrechts. Denn nach bisheriger deutscher Rechtslage genügte

es, wenn eine geheime Tatsache von kommerziellem Wert nach dem erkennbaren subjektiven Willen des Inhabers geheim gehalten werden soll. Getreu dem Motto „handeln, nicht wünschen“ reicht also der bloße Wille des Informationsinhabers nicht mehr aus. Er muss auch angemessene Maßnahmen zum Schutz der Informationen ergreifen. Hier ist in prozessualer Hinsicht zu beachten, dass das objektive Merkmal „Maßnahme“ dann auch im Streitfall vom Informationsinhaber zu beweisen ist. Beispiele für solche Maßnahmen sind physische Zugangsbeschränkungen und vertragliche Sicherungsmechanismen. Bedeutung erlangen hier insbesondere Geheimhaltungsvereinbarungen mit externen Vertragspartnern sowie Vertraulichkeitsvereinbarungen mit Mitarbeitern.

Erlaubte Handlungen im Umgang mit Geschäftsgeheimnissen

Was im Hinblick auf Geschäftsgeheimnisse erlaubt ist, wird durch die in § 2 GeschGehG genannten Fallgruppen geregelt. Hierzu zählen zunächst nach § 2 Abs. 1 GeschGehG Handlungen durch Gesetz oder die auf Grund eines Gesetzes erfolgen. Aber auch die Erlangung, Nutzung oder Offenlegung durch Rechtsgeschäft sind hiernach erlaubt.

Interessanter, weil unklarer, sind die Erlaubnistatbestände des Abs. 2. Das „insbesondere“ zu Beginn der Aufzählung dürfte so zu lesen sein, dass die danach aufgezählten Fallgruppen als Konkretisierung der gesetzlichen Erlaubnis (eben aufgrund des GeschGehG) zu verstehen sind. Nicht ausgeschlossen ist aber, dass dies eine Öffnungsklausel für bisher von der Rechtsprechung anerkannte oder zukünftig anzuerkennende, ungeschriebene Erlaubnissituationen darstellen soll. Geschützt sind hierüber eigenständige Entdeckungen oder Schöpfungen (Nr. 1) sowie – unter bestimmten zusätzlichen Voraussetzungen - das sog. „Reverse Engineering“, also die Entschlüsselung von Geschäftsgeheimnissen bzgl. Produkten aus den Produkten selbst. Hierdurch soll verhindert werden, dass Exklusivrechte an Informationen begründet werden, die als Geschäftsgeheim-

nisse geschützt sind; vielmehr soll dies dem Umstand Rechnung tragen, dass es im Fall der parallelen Entdeckung oder Schöpfung mehrere Inhaber ein und desselben Geschäftsgeheimnisses geben kann.

Nr. 2 lit. b) (rechtmäßige Besitz und keine Erlangungsbeschränkung) gibt dem Geheimnisinhaber dabei die Wahl, die Möglichkeit des Reverse Engineering vertraglich auszuschließen und so die Rechtmäßigkeit der Erlangung zu verhindern oder aber den Vertragspartner entsprechend gewähren zu lassen. Umgekehrt betrachtet bedarf es hier also einer aktiven Vertragsgestaltung durch den Geheimnisinhaber, wenn er das Reverse Engineering verhindern möchte.

In Nr. 3 ist klargestellt, dass Unternehmen keine Mitbestimmungs- und Arbeitnehmerrechte durch Berufung auf vermeintliche Geschäftsgeheimnisse beschränken können. Arbeitsrechtliche Geheimhaltungsvereinbarungen bleiben nach der Entwurfsbegründung hiervon unberührt.

Verbotene Handlungen

Eine der zentralen Vorschriften ist § 3 GeschGehG, welcher die in Bezug auf Geschäftsgeheimnisse verbotenen Handlungen regelt. Dabei ist § 3 GeschGehG stets zusammen mit § 4 GeschGehG zu prüfen, da dieser die Situationen regelt, in denen ein Verstoß gegen die Handlungsverbote ausnahmsweise gerechtfertigt ist.

Abs. 1 Nr. 1 des Verbotskatalogs zählt abschließend die verschiedenen verbotenen Handlungsarten sowie Handlungsobjekte bzgl. der Erlangung von Geschäftsgeheimnissen auf. Nr. 2 des ersten Absatzes stellt einen Auffangtatbestand dar und birgt als solcher bis zum Ergehen erster ober- und höchstrichterlicher Rechtsprechung erhebliche Rechtsunsicherheit für die Beteiligten. Der zweite Absatz hingegen normiert die Fälle, in denen eine Offenlegung verboten ist. Zu guter Letzt soll Abs. 3 Situationen erfassen, in denen beispielsweise die Person, welche das Geschäftsgeheimnis erlangt hat, selbst keinen Verstoß im Sinne des Abs. 2 begangen hat, aber das Geheimnis von einem Dritten erhalten hat. In diesem Fall kommt es auf den Vorsatz bzw. die grob fahrlässige Unkenntnis dieser Person an.

Rechtfertigung von Verstößen gegen Handlungsverbote

Eine Handlung, die nach § 3 des GeschGehG verboten ist, kann jedoch nach § 4 ausnahmsweise gerechtfertigt sein, wenn dies „zum Schutz eines berechtigten Interesses“ erfolgt. Als

solches gilt nach der Entwurfsbegründung jedes von der Rechtsordnung gebilligte Interesse, also auch ein wirtschaftliches oder ideelles, soweit es in diesem Sinne gebilligt ist. Diese offene Formulierung dürfte eine Interessenabwägung im Einzelfall erforderlich machen.

Der § 4 enthält sodann eine nicht abschließende („insbesondere“) Aufzählung von Fällen, in denen die verbotene Erlangung, Nutzung oder Offenlegung eines Geschäftsgeheimnisses zum Schutze berechtigter Interessen erforderlich sein kann. § 4 Nr. 2 GeschGehG-E dient ausweislich der Entwurfsbegründung explizit dem verstärkten Schutz von „Whistleblowern“. Daher war diese Norm bislang auch häufigster Gegenstand der bislang vernehmbaren kritischen Stellungnahmen zum Entwurf des GeschGehG. Kritisiert wurde hier insbesondere die Tatsache, dass als Voraussetzung der Rechtfertigung die „Absicht“ geregelt wird, das öffentliche Interesse zu schützen, da dies die Fälle aus dem Anwendungsbereich fallen lasse, in denen der Whistleblower zwar nicht altruistisch handle, die Aufdeckung jedoch trotzdem im Interesse der Allgemeinheit stehe. Als Beispiele für die in der Norm genannten „Fehlverhalten“ nennt die Entwurfsbegründung unethische Auslandsaktivitäten wie Kinderarbeit sowie auch gesundheitsschädliche oder umweltschädliche Produktionsbedingungen.

Ansprüche des Geschäftsgeheimnisinhabers bei Rechtsverletzungen

Jedes Verbot ist nur so wirksam wie die Sanktionen für einen entsprechenden Verstoß dagegen. Daher sieht der Entwurf des GeschGehG eine Reihe von Ansprüchen des Inhabers von Geschäftsgeheimnissen vor, die im Falle von (nicht nach § 4 gerechtfertigten) Verstößen gegen Handlungsverbote gegen den Verletzer geltend gemacht werden können.

Zu diesen Ansprüchen zählen:

- Beseitigung und Unterlassung (§ 5),
- Vernichtung, Herausgabe, Rückruf, Entfernung bzw. Rücknahme vom Markt (§ 6)
- Auskunft über rechtsverletzende Produkte sowie Schadensersatz im Falle falscher oder nicht erfolgter Auskunft (§ 7),
- Schadensersatzanspruch bei Verletzungen eines Geschäftsgeheimnisses (§ 9)

Ansprüche des Geschäftsgeheimnisinhabers bei Rechtsverletzungen

§ 5 Beseitigung und Unterlassung

§ 6 Vernichtung, Herausgabe, Rückruf, Entfernung bzw. Rücknahme vom Markt

§ 7 Auskunft über rechtsverletzende Produkte sowie Schadensersatz im Falle falscher oder nicht erfolgter Auskunft

§ 9 Schadensersatzanspruch bei Verletzungen eines Geschäftsgeheimnisses

Zudem besteht die Möglichkeit, einen etwaigen Anspruch nach §§ 5 – 7 unter bestimmten Voraussetzungen auch gegen den Inhaber eines Unternehmens zu richten, bei dem der Rechtsverletzer Beschäftigter ist.

Ihre Schranken finden diese Ansprüche insbesondere

- im Ausschluss der Ansprüche gem. §§ 5 – 7 bei Unverhältnismäßigkeit (§ 8),
- in der Möglichkeit des Rechtsverletzers, einen Anspruch nach den §§ 5 oder 6 durch Zahlung einer Geldabfindung abzuwenden (§ 10)
- sowie im allgemeinen Verbot der missbräuchlichen Geltendmachung der Ansprüche (§ 13).

Flankiert werden diese zivilrechtlichen Ansprüche von der Strafvorschrift des § 22, welcher dem Regelungsgehalt der bisherigen §§ 17 – 19 UWG entspricht. Ausweislich der Entwurfsbegründung soll ausdrücklich auch das „Whistleblowing“ gestärkt werden, indem entsprechende Situationen vielfach aus dem Anwendungsbereich der Strafvorschrift herausfallen sollen.

Unser Kommentar

Es bleibt abzuwarten, welche Änderungen sich am bisherigen Entwurfsstand bis zum Inkrafttreten eines finalen deutschen GeschGehG noch ergeben werden. Mit Spannung zu erwarten ist insbesondere die Beantwortung der Frage, ob die im gegenwärtigen Entwurf vorhandenen Abweichungen von der EU-Richtlinie in der Umsetzung weiterhin bestehen bleiben. Es steht zu erwarten, dass im Zuge der bereits ergangenen, teils sehr kritischen Stellungnahmen der betroffenen Kreise weitere Änderungen an dem Entwurf vorgenommen werden.



Unser Web-Tipp:

Weiter Infos zum Thema finden Sie auf www.know-how-richtlinie.de

BGH: Bonusaktion für Smartphone-App „My Taxi“

Die Bonusaktion „My Taxi“, bei der von dem Taxikunden nur die Hälfte des regulären Fahrpreises zu zahlen ist, ist auch unter Berücksichtigung der tariflichen Preisbindung zulässig. Der Bundesgerichtshof hat die Bonusaktion der Smartphone-App „My Taxi“ nicht beanstandet und die Klage der Taxizentralen abgewiesen.

■ Urteil vom 29. März 2018, Az.: I ZR 34/17

Hintergrund

Die Klägerin ist ein genossenschaftlicher Zusammenschluss von mehreren Taxizentralen aus Deutschland, welche die Taxi-Bestell-App „Taxi Deutschland“ betreiben. Die Beklagte vermittelt Taxi-Dienstleistungen über die Smartphone-App „My Taxi“.

Die Klägerin wendet sich gegen vier Bonusaktionen der Beklagten, bei denen der registrierte Nutzer lediglich die Hälfte des regulären Fahrpreises zahlen musste, während die andere Hälfte des Fahrpreises abzüglich einer Vermittlungsgebühr von der Beklagten bezahlt wurde. Die Klägerin nimmt die Beklagte auf Unterlassung in Anspruch und begründet dies mit einem Verstoß gegen die Pflicht zur Einhaltung der behördlich festgesetzten Taxitarife. Das Landgericht hat der Klage stattgegeben und auch die Berufung der Beklagten hatte keinen Erfolg. Mit der Revision vor dem Bundesgerichtshof verfolgt die Beklagte ihren Antrag auf Abweisung der Klage.

Die Entscheidung

Der Bundesgerichtshof hat der Revision stattgegeben und die Klage abgewiesen. Die Bonusprogramme der Beklagten verstießen nicht gegen die tarifliche Preisbindung für Taxiunternehmen, da die Beklagte selbst kein Taxiunternehmen ist, für die die Festpreise gelten. Die Tätigkeit der Beklagten beschränkt sich vielmehr auf die Vermittlung von Fahraufträgen, die von unabhängigen Taxiunternehmen selbstständig durchgeführt werden. Den Taxiunternehmen steht es frei die Dienste anderer Vermittler in Anspruch zu nehmen oder sich auch der Klägerin anzuschließen.

Der Bundesgerichtshof äußert sich darüber hinaus aber auch zu den Bonusprogrammen an sich. Grundsätzlich sind die Bestimmungen der § 51 Abs. 5, § 39 Abs. 3 Personenbeförderungsgesetz (PBefG) Marktverhaltensregeln im Sinne von § 3a des Gesetzes gegen unlauteren Wettbewerb (UWG). Das bedeutet, dass bei einem Verstoß ein Vorgehen nach dem UWG möglichst ist und insbesondere Beseitigung, Unterlassen und Schadensersatz verlangt werden kann.

Grundsätzlich dürfen die festgesetzten Beförderungsentgelte nicht über- oder unterschritten werden. Insbesondere sind Er-

mäßigungen, die nicht unter gleichen Bedingungen jedermann zugutekommen, verboten und nichtig. Daraus folgt, dass der Taxiunternehmer keinen Nachlass auf den tariflichen Festpreis gewähren darf. Jedoch liegt kein Verstoß gegen die Tarifpflicht vor, wenn der Festpreis vollständig an ihn gezahlt wird. Ein Verstoß gegen die Tarifpflicht liegt dann nicht vor, wenn das Vermögen des Taxiunternehmers nach Beförderung des Fahrgastes in Höhe des Festpreises vermehrt wird. Die Zahlungspflicht der Provision der Beklagten vermindert den Festpreis nicht, sondern ist allein eine zulässige Vergütung ihrer Vermittlungsleistungen. Sofern argumentiert wird, dass Sinn und Zweck der Tarifpflicht durch die Bonusaktionen unterwandert wird, sieht der Bundesgerichtshof die Funktionsfähigkeit des Taxiverkehrs durch die Bonusaktionen nicht als gefährdet an. Vielmehr soll solange den Taxiunternehmen ausreichende Vermittlungsmöglichkeiten zur Verfügung stehe kein Grund bestehen, den Wettbewerb im Bereich der Taxivermittlung einzuschränken.

Letztlich sieht der Bundesgerichtshof auch keine gezielte Behinderung der Klägerin durch die Beklagte gem. § 4 Nr. 4 UWG. Die nicht kostendeckende Erbringung einer Dienstleistung ist danach nur unter bestimmten Voraussetzungen verboten, insbesondere dann, wenn sie zur Verdrängung von Mitbewerbern geeignet ist und in Verdrängungsabsicht erfolgt. Aufgrund der zeitlichen und örtlichen Begrenzung dieser Aktion fehlt aber eine Eignung zur Verdrängung von Mitbewerbern. Entgegen der Entscheidung der Vorinstanz sieht der Bundesgerichtshof keinen Wettbewerbsverstoß an sich und ordnet die Tätigkeit der Beklagten auch nicht als eine Anstiftung oder sonstige Teilnahme bei einem Wettbewerbsverstoß ein.

Unser Kommentar

Durch diese Entscheidung des Bundesgerichtshofs werden Rabattaktionen im regulierten Umfeld des Personenbeförderungsgesetzes ermöglicht. Die Argumentation des Bundesgerichtshofs kann insofern bei dem Entwurf derartiger Rabattaktionen als Blaupause dienen. In diesem Zusammenhang ist zu beachten, dass der Koalitionsvertrag eine Modernisierung des Personenbeförderungsgesetzes vorsieht, um digitale Mobilitätsangebote zu ermöglichen. Insofern könnte diese Entscheidung als eine erste Leitlinie verstanden werden.

BGH: Bei offensichtlichen (Urheber-)Rechtsverletzungen sind Internet-Provider zur Speicherung von Daten verpflichtet

Mit seinem Urteil vom 21. September 2017 hat der Bundesgerichtshof bestätigt, dass Access-Provider verpflichtet sind, bereits rechtmäßig erhobene Verkehrsdaten (z.B. dynamische IP-Adressen und deren Zuordnung zu Kunden) nicht zu löschen, bis ein bereits angestregtes Gestattungsverfahren bzgl. der Verwendung von Verkehrsdaten für eine Auskunftserteilung in Zusammenhang mit offensichtlichen Rechtsverletzungen (durch Nutzer des Access-Service) abgeschlossen ist, soweit diese Verkehrsdaten die Erteilung der Auskunft ermöglichen.

■ Urteil vom 21. September 2017, Az.: I ZR 58/16

Hintergrund

Das Urhebergesetz (UrhG) sieht in § 101 Absatz 2 Satz 1 Nr. 3 vor, dass in Fällen offensichtlicher Rechtsverletzungen sowie in Fällen, in denen der Verletzte gegen den Verletzer bereits Klage erhoben hat, ein Auskunftsanspruch nicht nur den Verletzer trifft, sondern grundsätzlich auch gegen den Dienstleister gerichtet werden kann, der in gewerblichem Ausmaß Dienstleistungen erbringt, die für die rechtsverletzende Tätigkeit genutzt wurden. In der Praxis wird dieser Auskunftsanspruch regelmäßig gegenüber (Internet-)Access-Providern geltend gemacht, über deren Internet-Zugang z.B. Musik-, Film-, Game- und e-Book-Kopien urheberrechtswidrig mittels File-Sharing-

Software angeboten wird. Gegenstand des Auskunftsanspruchs sind dabei insbesondere die Zuordnungen dynamischer IP-Adressen zu Kunden des Access-Providers und deren Anschriften. Da es sich hierbei um Verkehrsdaten im Sinne des § 3 Nr. 30 Telekommunikationsgesetz (TKG) handelt, ist gem. § 101 Absatz 9 Urhebergesetz eine richterliche Anordnung über die Zulässigkeit der Verwendung dieser Verkehrsdaten erforderlich. Der Verletzte kann diese beantragen (das sogenannte Gestattungsverfahren).

Im vorliegenden Fall hatte ein Tonträgerhersteller einen Access-Provider, der seinen Kunden Zugang zum Internet unter Verwendung dynamischer IP-Adressen bietet, nach entsprechen-

der außergerichtlicher Aufforderung insbesondere gerichtlich in Anspruch genommen, die Löschung konkret benannter Datensätze zu unterlassen. Bei den Datensätzen handelte es sich Verbindungsdaten zu IP-Adressen des Access-Providers mit den zugehörigen Verbindungszeitpunkten. Zu den angegebenen Zeitpunkten sollen die Nutzer, denen der Access-Provider diese Ad-



ressen vorübergehend zugewiesen hatte, mittels einer File-Sharing-Software angeblich Musikaufnahmen zum Download angeboten haben, an denen der Tonträgerhersteller ausschließliche Verwertungsrechte geltend macht.

Die Entscheidung

Die Entscheidung des Bundesgerichtshofs deckt zwei rechtliche Themenkomplexe ab. Zum einen hat der Bundesgerichtshof klargestellt, dass für einen Antrag auf Löschungsuntersagung bzgl. Daten, die dem Antragsgegner die Auskunftserteilung nach § 101 Absatz 2 Satz 1 Nr. 3 UrhG ermöglichen, der Rechtsweg zur streitigen ordentlichen Gerichtsbarkeit eröffnet ist. Zum anderen hat der Bundesgerichtshof entschieden, dass die hier von dem Tonträgerhersteller ersuchte Löschungsuntersagung grundsätzlich begründet sein kann, da eine Verpflichtung des (Internet-) Access-Providers besteht, in Fällen offensichtlicher Rechtsverletzungen bis zum Abschluss des Gestattungsverfahrens nach § 101 Absatz 9 UrhG die Löschung des Access-Providers nach § 96 Absatz 1 Satz 1 TKG rechtmäßig erhobenen Verkehrsdaten zu unterlassen, die die Auskunftserteilung nach § 101 Absatz 2 Satz 1 Nr. 3 UrhG ermöglichen.

Hintergrund ist der Umstand, dass diese Löschungsuntersagung der Sicherung des gesetzlichen Auskunftsanspruchs gegen Dienstleister des Verletzers diene. Dieser sei selbst wiederum ein Hilfsanspruch zur Vorbereitung von Unterlassungsansprüchen und Schadensersatzansprüchen gegen den Verletzer. Der Bundesgerichtshof begründet dies mit dem Sinn und Zweck der EU-Richtlinie (2004/48/EG), welche durch den Auskunftsanspruch im Urhebergesetz umgesetzt wurde. Voraussetzung sei dabei aber in jedem Fall, dass der Access-Provider vor der Löschung der entsprechenden Daten vom Verletzten auf eine Rechtsverletzung aufmerksam gemacht worden sei. Dem stehe auch nicht entgegen, dass Verkehrsdaten (wie z.B. die hier relevanten Informationen zu den dynamischen IP-Adressen) besonderen Schutz nach dem Telekommunikationsgesetz genießen. Denn es ergäbe sich aus der Natur der Sache, dass eine Löschung der benötigten Daten vorläufig unterbleiben dürfe und müsse, soweit die Daten für die Auskunftserteilung erforderlich seien, der das Gestattungsverfahren vorangestellt sei, das den Richtervorbehalt umsetzt.

Unser Kommentar

Der Auskunftsanspruch des § 101 Absatz 2 Satz 1 Nr. 3 UrhG gegen Dritte, die in gewerbsmäßigen Ausmaß Dienstleistungen erbringen, welche von dem Verletzer für seine rechtsverletzenden

de Tätigkeit genutzt werden, unterliegt engen Grenzen – bis hin zum Verhältnismäßigkeitsvorbehalt des § 101 Absatz 4 UrhG. Im Hinblick auf Internet-Access-Provider ist insbesondere der Richtervorbehalt des § 101 Absatz 9 UrhG zu betonen. Der Richtervorbehalt bestimmt, dass der Verletzte eine vorherige richterliche Anordnung benötigt, wenn die Auskunft die Verwendung von Verkehrsdaten im Sinne des Telekommunikationsgesetzes erfordert – also u.a. immer, wenn dynamische IP-Adressen betroffen sind. Damit wird einerseits der besondere Schutz der Telekommunikationsdaten sichergestellt und andererseits der Access-Provider davon entlastet, selbst zu prüfen, ob eine offensichtliche Rechtsverletzung vorliegt. Kehrseite hiervon ist der damit notwendige zusätzliche Schritt für die Verletzten bei der Umsetzung des Auskunftsanspruchs und das Risiko, dass durch diesen Schritt eine weitere Verzögerung eintritt. Dieser zusätzliche Schritt kann auch dazu führen, dass der Auskunftsanspruch ins Leere geht, falls der Access-Provider die Verkehrsdaten bereits gelöscht hat, wenn der Auskunftsanspruch geltend gemacht wird. Bei der Geltendmachung von Auskunftsansprüchen gegen gewerbliche Dienstleister, wie (Internet-)Access-Provider, ist daher grundsätzlich ein schnelles Handeln geboten. Mit seiner aktuellen Entscheidung bestätigt der Bundesgerichtshof eine diese Situation erleichternde „Erweiterung“ des Arsenal der Rechteinhaber zur besseren Wahrung ihrer Rechte.

Sowohl Rechteinhaber als auch Access-Provider sollten ihre Standardabläufe nunmehr kurzfristig entsprechend anpassen. Rechteinhaber sollten zeitgleich mit dem Gestattungsverfahren nach § 101 Absatz 9 UrhG zukünftig die relevanten Access-Provider umgehend unter Verweis auf das Gestattungsverfahren informieren und auffordern, die entsprechenden (dabei konkret zu benennenden) Daten nicht zu löschen, soweit sie das Risiko einer Löschung sehen. Access-Provider sollten wiederum sicherstellen, dass entsprechende Aufforderungen, die bei ihnen eingehen, umgehend an die relevanten internen Stellen weitergeleitet werden, um diese zu prüfen und die (wie der Bundesgerichtshof nunmehr bestätigt hat) ggf. dann verpflichtende Unterlassung der Löschung sicherzustellen. Zugleich ist auf Seiten der Access-Provider jedoch auch sicherzustellen, dass die entsprechenden Daten nicht unbefristet gespeichert werden, sondern zu gegebener Zeit (insbesondere falls im Gestattungsverfahren die Erteilung der richterlichen Anordnung nicht erfolgt) gelöscht werden, um den entsprechenden gesetzlichen Pflichten auch insoweit nachzukommen.

Veranstaltungen und Veröffentlichungen



Eine Übersicht mit unseren Veranstaltungen finden Sie [hier](#)



Eine Liste unserer aktuellen Veröffentlichungen finden Sie [hier](#)

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22
50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Copyright: Alle Texte dieses Newsletters sind urheberrechtlich geschützt. Gerne dürfen Sie Auszüge unter Nennung der Quelle nach schriftlicher Genehmigung durch uns nutzen. Hierzu bitten wir um Kontaktaufnahme. Falls Sie künftig keine Informationen der Luther Rechtsanwaltsgesellschaft mbH erhalten möchten, senden Sie bitte eine E-Mail mit dem Stichwort „IP/IT“ an unsubscribe@luther-lawfirm.com

Bildnachweis: Fabrika/Fotolia: Seite 1; Julien Eichinger/Fotolia: Seite 4; Carlos Amarillo/Shutterstock.com: Seite 7; digitalstock: Seite 9

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapur, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com.



Auf den Punkt. Luther.

