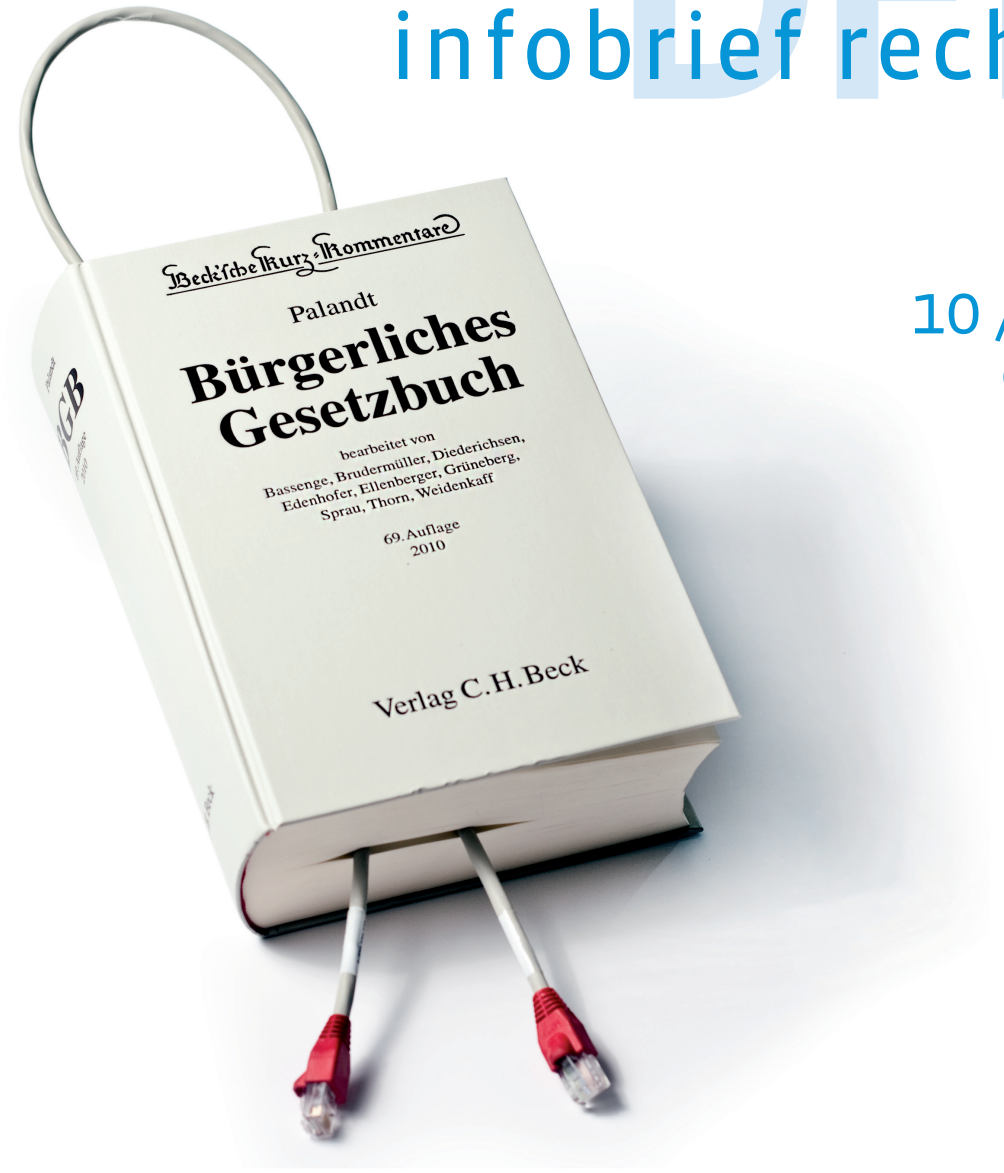
DEN infobrief recht



10 / 2018
Oktober 2018

Zugang gesperrt! Bitte nicht stören!
Der BGH zur unionsrechtskonformen Auslegung des neuen Telemediengesetzes

Kriminelles Schürfen im Cyberspace
BGH verurteilt Betreiber eines Botnetzes, welches zur Bitcoin-Erzeugung eingesetzt wurde

Hochschulen betreiben kein Gewerbe, sind aber Gewerbetreibende
EuGH stärkt den Verbraucherschutz bei der Kreditvergabe durch Hochschulen

Zugang gesperrt! Bitte nicht stören!

Der BGH zur unionsrechtskonformen Auslegung des neuen Telemediengesetzes

von Johannes Baur

Die „Abschaffung der Störerhaftung“ für Internetzugangsvermittler feiert in diesem Monat ihr einjähriges Jubiläum. Viel Diskussionsbedarf bestand bezüglich der stattdessen eingeführten Möglichkeit zur verpflichtenden Einrichtung von Netzsperren. Unter anderem wurde die Vereinbarkeit der neuen Regelung mit den Vorgaben des Unionsrechts angezweifelt. Diese Zweifel räumt der Bundesgerichtshof (BGH) nun in einem aktuellen Urteil vom 26.07.2018 (Az.: I ZR 64/17) aus. Interessant dabei ist, dass das Gericht den Kreis der Anspruchsgegner für die Einrichtung von Netzsperren im Wege einer richtlinienkonformen Rechtsfortbildung über den Wortlaut hinaus ausdehnt.

I. Netzsperren als Substitution für die Störerhaftung

Der Internetzugang von Hochschulen und Forschungseinrichtungen steht einer Vielzahl von Mitarbeitern, Studierenden und Gästen aus Wissenschaft und Forschung offen. Im Regelfall wird er dabei zu legalen Zwecken eingesetzt. Es ist jedoch nicht ausgeschlossen, dass sich unter den Nutzern schwarze Schafe befinden, die den universitären Internetzugang für die Verletzung von Rechten des geistigen Eigentums missbrauchen. Manch Studierender oder Mitarbeiter tätigt beispielsweise auf Tauschbörsen illegale Up- oder Downloads von Musikstücken, Filmen oder Computerspielen. Nicht selten flatterte daher auch Hochschulen und Forschungseinrichtungen in der Vergangenheit Post vom Anwalt ins Haus, wobei entweder Auskunft über die Daten des konkreten Nutzers verlangt oder die Unterlassung weiterer Rechtsverletzungen gefordert wurde. Während Verkehrsdaten, welche Aufschluss über den konkreten Rechtsverletzer geben könnten, nicht (langfristig) protokolliert werden und eine Auskunft daher nicht möglich ist, stellte sich die Frage, wie mit der Aufforderung zur Abgabe von strafbewährten Unterlassungserklärungen und der Geltendmachung von damit einhergehenden Abmahnkosten umzugehen sei. Auch wenn der tatsächliche Rechtsverletzer nicht zu ermitteln war, blieb offen, ob die Hochschule oder Forschungseinrichtung als Zugangsvermittler für die Verletzung eine Mitverantwortung trägt. Eine solche Haftung des „Zugangsvermittlers“ wurde nach alter Rechtslage von der Rechtsprechung nach den Grundsätzen der „Störerhaftung“ angenommen. Störer war dabei derjenige, der – ohne selbst Täter oder Teilnehmer zu sein – willentlich und adäquat-kausal zur Rechtsverletzung beitrug. Daraus folgte, dass Zugangsanbieter für die Rechtsverletzung ihrer Nutzer zur Verantwortung gezogen werden konnten, wenn sie keine zumutbaren und verkehrsüblichen Vorkehrungen trafen, um Rechtsverletzungen zu verhindern.

Die Störerhaftung war bei Zugangsanbietern, insbesondere bei Betreibern öffentlicher WLAN-Hotspots, verständlicherweise unbeliebt. In Anbetracht des Haftungsrisikos waren viele Betreiber davor zurückgeschreckt, einen eigenen Zugang anzubieten. Dem wollte der Gesetzgeber begegnen und normierte im zweiten Anlauf im Oktober 2017 durch das 3. Telemedienänderungsgesetz schließlich die „Abschaffung der Störerhaftung“.[1] Nach § 8 Abs. 1 S. 2 Telemediengesetz (TMG) sind Ansprüche auf Schadensersatz, Beseitigung und Unterlassung sowie damit einhergehende Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche gegen

1 Siehe dazu bereits ausführlich, Klein, Wer hat noch nicht, wer will noch mal?, DFN-Infobrief Recht 11/2017.

Zugangsvermittler nun ausdrücklich ausgeschlossen. Um die Rechteinhaber nicht schutzlos stehen zu lassen, wurde im Gegenzug in § 7 Abs. 4 TMG gegen die Anbieter drahtloser Netzwerke ein Anspruch auf die Einrichtung von Netzsperren geschaffen. Vor- und außergerichtliche Kosten für die Durchsetzung dieses Anspruchs dürfen von den Rechteinhabern hingegen nicht verlangt werden.

Auch die neue Regelung sah sich Kritik ausgesetzt, da die Befürchtung bestand, die Rechteinhaber könnten unangemessen benachteiligt sein. Die EU-Urheberrechtsrichtlinie (InfoSoc-RL) und die Unionsrichtlinie zur Durchsetzung der Rechte des geistigen Eigentums (Enforcement-RL) sehen vor, dass die Mitgliedstaaten gerichtliche Anordnungen gegen Zugangsvermittler ermöglichen müssen. Gestützt wird dies durch den Schutz des geistigen Eigentums in der EU-Grundrechtecharta. Es bestanden Zweifel darüber, ob die neuen nationalen Vorschriften in der Lage sind, diesen Anforderungen des Unionsrechts, die den Interessen der Rechteinhaber an der Durchsetzung ihrer Ansprüche dienen, gerecht zu werden. Der BGH hat sich nun in einer aktuellen Entscheidung zu diesen Fragen positioniert. Dabei kommt er zum Ergebnis, dass die Abschaffung der Störerhaftung grundsätzlich unionsrechtskonform ist. Bezüglich der Reichweite der Anwendung der Sperrverpflichtung sieht er jedoch Bedarf für eine richtlinienkonforme Rechtsfortbildung.

II. Der Sachverhalt

Der Beklagte ist Inhaber eines Internetanschlusses, über den fünf öffentlich zugängliche WLAN-Hotspots und zwei drahtgebundene „Tor-Exit-Nodes“ betrieben werden. Bei einem Tor-Exit-Node handelt es sich um die Schnittstelle, welche die Kommunikation aus dem verschlüsselten TOR-Netzwerk ins „gewöhnliche Internet“ weiterleitet. Das TOR-Netzwerk dient der Anonymisierung von Verbindungsdaten.

Über den Internetanschluss des Beklagten wurden am 6. Januar 2013 Teile des Computerspiels „Dead Island“ auf einer Tauschbörse im Internet zum Download angeboten. Es ließ sich dabei nicht klären, ob dies über die WLAN-Hotspots oder die drahtgebundenen Tor-Exit-Nodes geschah. Die Klägerin ist Inhaberin der ausschließlichen Nutzungsrechte am betroffenen Computerspiel und mahnte den Beklagten mit Schreiben vom 14. März 2013 ab. Außerdem forderte sie die Abgabe einer strafbewährten Unterlassungserklärung. Bereits im Jahr 2011 war der Beklagte von der Klägerin zweimal wegen Urheberrechtsverletzungen durch Filesharing abgemahnt worden. Als der Beklagte sich weigerte, legte die Klägerin erfolgreich Klage vor dem Landgericht Düsseldorf ein. Die Berufung zum Oberlandesgericht Düsseldorf blieb erfolglos. Mit der Revision zum BGH möchte die Beklagte die Abweisung der Klage erreichen. Der BGH wies dieses Ersuchen bezüglich der Abmahnkosten zwar ab, gab ihm bezüglich des Unterlassungsanspruchs aber statt.

III. Die Entscheidung des BGH

Der BGH stellt zunächst fest, dass die von der Klägerin geltend gemachten Abmahnkosten nicht zu beanstanden sind. Voraussetzung für die Geltendmachung von Abmahnkosten sei, dass zum Zeitpunkt der Abmahnung ein materieller Unterlassungsanspruch zugrunde gelegen hat und somit die Abmahnung dem Schuldner die Möglichkeit eröffnet, die Sache ohne eine gerichtliche Entscheidung beizulegen. An den Nutzungsrechten der Klägerin am Computerspiel sowie an der über den Internetanschluss des Beklagten begangenen Rechtsverletzung bestehen, nach Ansicht des BGH, keine Zweifel. Dass diese vom Beklagten selbst begangen wurde, ließe sich zwar nicht nachweisen, jedoch läge eine Haftung für durch Dritte begangene Rechtsverletzungen vor. Zum Zeitpunkt der Abmahnung galt das TMG noch in seiner Fassung vom 26. Februar 2007. Die Grundsätze der Störerhaftung waren demnach noch anwendbar. Nach diesen sei der Anschlussbetreiber bezüglich des WLAN-Hotspots zur Vornahme verkehrsüblicher und zumutbarer Zugangssicherungen verpflichtet gewesen. Dabei nennt das Gericht insbesondere die Einrichtung einer Passwortsperre für das WLAN. Auch bei Betrieb eines Tor-Exit-Nodes seien geeignete Sicherungsmaßnahmen möglich, wie die Einrichtung einer Port-Sperre für Tauschbörsen. Diesen Verpflichtungen sei der Beklagte nicht nachgekommen, wodurch der Anspruch auf Zahlung der Abmahnkosten bestehe.

Etwas anderes gelte dagegen für den ebenfalls geltend gemachten Unterlassungsanspruch. Dieser bestehe nur dann, wenn eine Wiederholungsgefahr gegeben ist. Eine solche sei aber abzulehnen, wenn in Zukunft keine Rechtsverletzung mehr zu erwarten ist. Durch die zwischenzeitliche Änderung des TMG werde der von der Klägerin geltend gemachte Unterlassungsanspruch für die Zukunft ausgeschlossen. Stattdes-

sen habe der Rechteinhaber nun die Möglichkeit, auf den nach § 7 Abs. 4 TMG möglichen Anspruch auf die Verpflichtung zur Einrichtung von Netzsperren zurückzugreifen. Dieser Anspruch besteht nach dem Wortlaut der Norm aber nur gegen WLAN-Betreiber. Im vorliegenden Fall war hingegen nicht ausgeschlossen, dass die Rechtsverletzung über das drahtgebundene TOR-Netzwerk erfolgte. Im Zweifel wäre zugunsten des Netzbetreibers hiervon auszugehen. Demnach müsste sowohl der Unterlassungsanspruch als auch der Sperranspruch entfallen.

Dieses Ergebnis hält der BGH für unionsrechtswidrig. Vor dem Hintergrund von Art. 8 Abs. 3 der InfoSoc-Richtlinie und Art. 11 S. 3 der Enforcement-Richtlinie dürfe der Rechteinhaber nicht schutzlos gestellt werden. Es müsse daher eine richtlinienkonforme Fortbildung des § 7 Abs. 4 TMG erfolgen. Demnach solle die Norm Anbieter drahtloser sowie drahtgebundener Netze gleichermaßen erfassen. Die unterschiedliche Art der Gewährung des Zugangs sei interessenneutral: ob der Zugang zu rechtswidrigen Inhalten über ein drahtgebundenes oder ein drahtloses Netz erfolgt, spiele weder für den Anschluss- noch den Rechteinhaber eine Rolle.

Auch zum Inhalt möglicher Sperrverpflichtungen äußerte sich der BGH. Grundsätzlich hält er Portsperren für die Unterbindung von Rechtsverletzungen über Tauschbörsen für geeignet. Jedoch gibt das Gericht zu bedenken, dass mögliche Sperrmaßnahmen vielfältig sein können. Zwar dürften Anschlussbetreiber, gem. § 8 Abs. 4 TMG, nicht durch Behörden zur Registrierung der Nutzer oder der Eingabe eines Passworts vor Gewährung des Zugangs oder zur dauerhaften Einstellung des Dienstes verpflichtet werden. Durch Gerichte dürften solche Maßnahmen aber durchaus aufgegeben werden, wenn keine milderen Mittel ersichtlich sind. Dabei müsse jedoch stets eine sorgfältige Abwägung mit den Grundrechten des Anschlussinhabers und der Nutzer erfolgen.

IV. Ausblick und Auswirkungen auf die Hochschulpraxis

„Die Störerhaftung ist abgeschafft!“ So oder so ähnlich lauteten die Schlagzeilen im vergangenen Jahr als Reaktion auf das 3. Telemedienänderungsgesetz. Diese euphorische Aussage ist jedoch mit Vorsicht zu genießen. Zwar ist die Haftung der Zugangsvermittler, die damals mit den Grundsätzen der Störerhaftung hergeleitet wurde, nach dem geltenden Recht tatsächlich passé. Durch die Schaffung eines Anspruchs auf Verpflichtung zur Einrichtung von Netzsperren sind die Anschlussinhaber aber auch nach der Gesetzesänderung nicht gänzlich aus dem Schneider. Begehen die Nutzer des Internetzugangs Verletzungen des geistigen Eigentums Dritter, können die Rechteinhaber von der Hochschule oder Forschungseinrichtung als Betreiber des Netzes verlangen, dass geeignete, verhältnismäßige und zumutbare Maßnahmen zur Sperrung der Nutzung der betroffenen Informationen eingerichtet werden, um eine Wiederholung der Rechtsverletzung zu verhindern. Dies gilt nach dem BGH nun ausdrücklich nicht nur für WLAN-Netze, sondern auch für drahtgebundene Internetzugänge. Über die Art der Sperren schweigt das Gesetz. Technisch denkbar sind DNS-, IP-, URL- und Port-Sperren. Auch wenn alle Netzsperren mehr oder weniger leicht zu umgehen sind, bedeutet dies nicht zwingend, dass sie deshalb nicht geeignet sind, um Wiederholungen der Rechtsverletzung zu verhindern. Auch die Erschwerung des Zugangs kann insoweit genügen. Technisch weniger versierte Nutzer können hierdurch von der Begehung der Taten abgehalten werden. Der BGH hält in seiner Entscheidung an der grundsätzlichen Eignung von Portsperren fest, wobei er deutlich macht, dass auch Zugangsbeschränkungen durch Passwörter oder - in Extremfällen - die komplette Sperrung des Zugangs erwartet werden können.

Vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes wird die Einrichtung umfassender Netzsperren oder eine Komplettsperrung des Zugangs von Hochschulen und Forschungseinrichtungen nicht erwartet werden können. Wird vom Rechteinhaber die Einrichtung einer Netzsperre gefordert, so müssen im Rahmen der Verhältnismäßigkeitsprüfung neben dem Recht des Verletzten am geistigen Eigentum auch die Grundrechtsposition der Nutzer in Gestalt der Informationsfreiheit und - im Wissenschaftsbetrieb - der Wissenschaftsfreiheit Berücksichtigung finden. Dabei sollten Hochschulen und Forschungseinrichtungen besonders sensibel vorgehen, um ein „Overblocking“ zu vermeiden. Keinesfalls darf eine Netzsperre soweit gehen, dass sie neben dem Zugriff auf den gemeldeten illegalen Inhalt auch den Zugriff auf legale Inhalte unterbindet.

Als Kompensation für diese Verpflichtung kam der Gesetzgeber den Hochschulen und Forschungseinrichtungen jedoch an anderer Stelle entgegen: die Gefahr der Inanspruchnahme für vor- und außergerichtlichen Kosten für die Durchsetzung des

Anspruchs auf Netzsperren besteht nicht. Rechteinhaber können für die reine Aufforderung zur Einrichtung der Netzsperre keine Kosten geltend machen. Wird der Zugangsanbieter auf die Rechtsverletzung aufmerksam gemacht und eine Netzsperre gefordert, so muss hingegen reagiert werden. Besteht nämlich der Anspruch auf Einrichtung der Netzsperre und verweigert sich die Hochschule oder Forschungseinrichtung einer Umsetzung, so müssen im Falle einer Niederlage vor Gericht die Gerichtskosten getragen werden. Es sollte daher jeweils in Abstimmung mit dem Justiziariat im Einzelfall entschieden werden, ob und welche Netzsperren verhältnismäßig sind.

Kriminelles Schürfen im Cyberspace

BGH verurteilt Betreiber eines Botnetzes, welches zur Bitcoin-Erzeugung eingesetzt wurde

von Matthias Mörike

Das Eindringen in fremde Computersysteme und deren Manipulation ist nicht nur ein Problem der IT-Sicherheit. Auch das Strafrecht kennt einige Normen, die bestimmte Handlungen in diesem Bereich sanktionieren und dadurch auch präventiv wirken sollen. Vor allem § 202a StGB (Ausspähen von Daten) und § 303a StGB (Datenveränderung) spielen dabei eine wichtige Rolle. Der Bundesgerichtshof (BGH) hat in seinem Beschluss vom 27. Juli 2017 (Az. 1 StR 412/16) den Betreiber eines Botnetzes unter anderem aufgrund dieser Straftatbestände verurteilt. Die Ausführungen des Gerichts wirken sich auch auf die Zulässigkeit von IT-Sicherheitsforschung aus.

I. Sachverhalt

Der Angeklagte betrieb mit einigen Mittätern ein sogenanntes Botnetz. Ein Bot ist ein Schadprogramm, das auf einem fremden Rechner unbemerkt von dessen Nutzer abläuft und bestimmte Befehle ausführen kann. Häufig werden auf vielen verschiedenen Rechnern Bots installiert, die sich über das Internet zu einem Botnetz verbinden. Die Bots empfangen ihre Befehle von einem Command-and-Control-Server mit der Folge, dass die fremden Rechner, wie auch im vorliegenden Fall geschehen, ferngesteuert werden können. Das Schadprogramm wird in der Regel als sogenannter Trojaner auf das fremde System geschleust. Im konkreten Fall wurde das Schadprogramm als vermeintlich harmlose Musik-, Video- oder Programmdatei getarnt und von ahnungslosen Nutzern von einer Internetseite heruntergeladen. Dadurch wurde das Programm unbemerkt installiert und konnte heimlich Verbindung zum Command-and-Control-Server aufnehmen, um dessen Befehle umzusetzen. Das so aufgebaute Botnetz wurde vom Angeklagten zum einen genutzt, um Daten der Nutzer und der infizierten Rechner auszuspähen und zu sammeln. Zum anderen nutzte er die ferngesteuerten Rechner, um Bitcoins zu schürfen. Diese virtuelle Währung kann dadurch erlangt werden, dass komplizierte Rechenaufgaben gelöst werden, die relativ große Mengen an Rechenleistung benötigen. Genau diese Rechnerkapazität erlangte der Angeklagte, indem er die fremden Rechner infizierte und entsprechende Befehle ausführen ließ.

II. Entscheidung des BGH

Dem Angeklagten wurde unter anderem vorgeworfen, sich durch die geschilderten Handlungen gemäß § 202a StGB (Ausspähen von Daten), § 303a StGB (Datenveränderung), § 263a StGB (Computerbetrug) und § 269 StGB (Fälschung beweiserheblicher Daten) strafbar gemacht zu haben. Aufgrund der Vielzahl von infizierten Rechnern lautete die Anklage hinsichtlich §§ 202a und 303a StGB auf Begehung in 245.534 und 327.379 Fällen. Da die Strafverfolgungsbehörden beim zentralen Command-and-Control-Server des Botnetzes eine Datenbank gefunden hatten, die genau auflistete, wie viele Systeme infiziert wurden, war eine solch genaue Beziffe-rung der Anzahl der Fälle möglich.

§ 202a StGB bestraft, wie bereits erwähnt, das Ausspähen von Daten. Dadurch wird – allgemein gesprochen – das Interesse geschützt, Daten geheim zu halten. Den Tatbestand verwirklicht, wer sich unbefugt Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Der Angeklagte hat sich demnach strafbar gemacht,

indem er die infizierten Dateien getarnt zum Download anbot, sodass die Nutzer die Schadsoftware unbewusst herunterluden und er dadurch Zugriff auf zahlreiche Daten der Rechner und der Nutzer erhielt.

Besonders interessant ist hier die Frage nach der Zugangssicherung und deren Überwindung. Dem BGH hat es als Zugangssicherung genügt, dass die angegriffenen Systeme (namentlich Microsoft-Betriebssysteme von Windows XP bis Windows 7) über eine integrierte und in der Voreinstellung aktivierte Firewall verfügen. Diese Firewall hätte, wenn die Schadsoftware nicht als harmlose Dateien getarnt worden und daher vom Nutzer installiert worden wäre, die Verbindung mit dem Command-and-Control-Server verhindert. Die Nutzer hätten die Firewall aber ungewollt außer Kraft gesetzt, indem sie der Installation aufgrund der Tarnung zugestimmt hätten. Dadurch wurde nach Auffassung des Gerichts die Firewall ausgeschaltet und damit eine Zugangssicherung im Sinne der Vorschrift überwunden. Verallgemeinert gesagt ist damit jede Art von Software, die mittels Täuschung des Nutzers eine auf dem System des Nutzers vorhandene und aktivierte Firewall umgeht und eigentlich durch diese abgewehrt worden wäre, ein Fall des § 202a StGB. Interessant ist an der Stelle auch, dass der BGH es beweisrechtlich billigte, dass bei einem Großteil (genaugenommen 75 %) der infizierten Systeme unterstellt werden durfte, dass die Firewall nach wie vor aktiviert war. Im Einzelfall konnte das nicht mehr nachgewiesen werden, da weder alle Betroffenen noch die Konfiguration der jeweiligen Systeme bekannt waren. Der Anteil von 75 % kam dadurch zustande, dass dem Angeklagten zugutegehalten werden musste, dass nicht alle Nutzer, sondern nur der Großteil eine funktionierende Firewall einsetzt. Angesichts allgemeiner Erfahrungswerte ist die Annahme von 75 % nach Auffassung des BGH tragfähig.

§ 303a StGB schützt im Gegensatz zu § 202a StGB nicht die Geheimhaltung von Daten, sondern das Interesse an der Richtigkeit und Verwendbarkeit von gespeicherten Daten. Daher wird derjenige bestraft, der rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Dabei werden nur Daten erfasst, bezüglich derer der Handelnde nicht verfügungsbefugt ist. Dadurch soll vermieden werden, dass man sich durch das Verändern eigener Daten strafbar macht. Für die Strafbarkeit nach § 303a StGB kommt es im vorliegenden Fall auf die genauen Abläufe an. Nach den Feststellungen des Instanzgerichts, dem Landgericht Kempten (LG Kempten), hat die Schadsoftware auf dem jeweiligen Rechner bewirkt, dass Einträge in der zentralen Registrierungsdatenbank des Systems, der sogenannten Registry-Datei, hinzugefügt wurden. Dadurch wurden die Schadprogramme bei jedem Systemstart automatisch geladen und ausgeführt. Die Tathandlung „verändern“ ist weit zu verstehen und umfasst jede Funktionsbeeinträchtigung von Daten durch Änderung ihres Informationsgehalts. Das hat der BGH hier in Bezug auf die zusätzlichen Einträge in der Registry-Datei bejaht. Durch das Hinzufügen würde sich das System anders verhalten als ohne die Änderung, nämlich die Schadsoftware automatisch laden und ausführen. Das genüge für eine Veränderung im Sinne der Vorschrift.

Die Strafbarkeit nach § 263a StGB (Computerbetrug) und § 269 StGB (Fälschung beweiserheblicher Daten) resultierte daraus, dass der Angeklagte für den Betrieb seines Botnetzes und für die weitere Verbreitung der Schadsoftware mehrere Server anmietete, dafür aber die Daten von bereits ausgespähten Nutzern verwendete und deren Konten belastete. § 263a StGB schützt das Vermögen und stellt deswegen Manipulation von Datenverarbeitungen unter Strafe, die zu einem Vermögensschaden führen. § 269 StGB will verhindern, dass rechtlich relevante Erklärungen, die aus Daten bestehen, gefälscht werden. Im vorliegenden Fall wurde dieser Straftatbestand durch die unrichtigen, elektronischen Anmieterklärungen verwirklicht. Darüber hinaus hat der BGH noch festgestellt, dass Bitcoins einer sogenannten Verfallsanordnung unterliegen können. Solche Anordnungen dienen dazu, die Vorteile, die ein Täter durch seine Taten erlangt (im vorliegenden Fall die Bitcoins), auszugleichen. Die Anordnung des BGH ist vor dem Hintergrund interessant, dass der rechtliche Charakter von Bitcoins noch nicht abschließend geklärt ist. Die Richter sahen aber als entscheidende Voraussetzung für eine Verfallsanordnung, dass das Erlangte einen materiellen, wirtschaftlichen Wert besitzt. Das sei bei Bitcoins der Fall.

III. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Der Beschluss des BGH verdeutlicht einmal mehr die strafrechtliche Relevanz von Botnetzen. Für Strafverfolgungsbehörden hat er zu einigen Vereinfachungen geführt. Insbesondere wurden die Darlegungslasten an einigen Punkten gesenkt, nachdem der BGH in einem früheren Beschluss die Beweiswür-

digung noch als unzureichend kritisiert hatte. Es ist beispielsweise zulässig, sich hinsichtlich der Frage, ob eine Firewall aktiviert ist, auf allgemeine Erfahrungswerte zu stützen.

Für die Praxis von wissenschaftlichen Einrichtungen hat der Beschluss ganz unterschiedliche Auswirkungen. Auf der einen Seite sollte beim Verdacht eines aktiven Botnetzes im eigenen Rechnersystem in Betracht gezogen werden, die Strafverfolgungsbehörden einzuschalten und Anzeige zu erstatten. Auf der anderen Seite ist umso größere Vorsicht geboten, falls zu wissenschaftlichen Zwecken ein Botnetz betrieben wird. Hier muss sorgfältig geprüft werden, ob strafbare Handlungen nach §§ 202a, 303a StGB erfolgen. Dass es im wissenschaftlichen Kontext nicht um die Erlangung von finanziellen Vorteilen geht, ist in diesem Zusammenhang irrelevant, da allein die Zugangsverschaffung beziehungsweise die Datenveränderung sanktioniert wird. Im Zweifel muss eine Einwilligung des Verfügungsberechtigten eingeholt werden, um die Strafbarkeit auszuschließen. Die Ausführungen des BGH zur Rolle einer Firewall als Zugangssicherung im Rahmen des § 202a StGB haben darüber hinaus Bedeutung für die gesamte IT-Sicherheitsforschung. Sofern eine Firewall aktiviert ist und die beabsichtigten Handlungen theoretisch unterbinden kann, ist deren Umgehung möglicherweise strafrechtlich relevant. Die genaue Art der Umgehung ist dabei nicht entscheidend. Im vorliegenden Fall genügte die Tarnung als harmlose Datei, um den Nutzer zu täuschen und damit auch die Firewall zu umgehen. Diese Ausführungen des Gerichts sollten bei der Konzeption entsprechender Forschungsprojekte und Testverfahren berücksichtigt werden.

Hochschulen betreiben kein Gewerbe, sind aber Gewerbetreibende

EuGH stärkt den Verbraucherschutz bei der Kreditvergabe durch Hochschulen

von Nico Gielen

Die Mitgliedstaaten der Europäischen Union haben sich dazu verpflichtet, ein hohes Verbraucherschutzniveau zu gewährleisten. Um dieses Ziel zu verwirklichen, hat die Europäische Union im Jahr 1993 die Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen (Richtlinie 93/13/EWG, im Folgenden: Klausel-RL) erlassen. Nach dieser Klausel-RL müssen die Mitgliedstaaten gewährleisten, dass missbräuchliche Klauseln nach deren jeweiliger Rechtsordnung unwirksam sind. Die Beurteilung, ob eine Klausel missbräuchlich ist, ist dabei zwar dem einzelnen Mitgliedstaat überlassen. Nach dem Urteil des Europäischen Gerichtshofs (EuGH) vom 17. Mai 2018 (Aktenzeichen C-147/16) muss aber jeder Mitgliedstaat auch in prozessualer Hinsicht sicherstellen, dass Klauseln in Verbraucherverträgen auf Missbräuchlichkeit überprüft werden. Dies gilt auch für unentgeltliche Darlehensverträge, die eine Universität mit ihren Studierenden abschließt.

I. Sachverhalt

Ausgangspunkt der Entscheidung des EuGH ist ein belgischer Rechtsstreit zwischen der Universität Antwerpen und einer ihrer Studentinnen. Da sich die Studentin nicht in der Lage sah, die Studienbeiträge zu zahlen, ließ sie sich von der Universität ein unentgeltliches Darlehen gewähren. Die Universität vereinbarte mit der Studentin, dass im Falle einer ausbleibenden Rückzahlung erhöhte Zinsen und eine Entschädigung anfallen. Nachdem die Studentin ihrer Rückzahlungspflicht nicht nachkam, wurde sie von der Universität verklagt, erschien allerdings nicht im gerichtlichen Termin. Aufgrund dieser sogenannten Säumnis der Beklagten entschied das Gericht zwar, dass die Studentin das Darlehen zurückzahlen müsse. Hinsichtlich der Forderung über die erhöhten Zinsen und die Entschädigung sah das Gericht mit Blick auf die Klausel-RL aber unionsrechtliche Fragen aufkommen und legte diese dem EuGH vor.

II. Entscheidung

Zunächst sollte der EuGH beantworten, ob das belgische Gericht trotz der Säumnis der beklagten Studentin prüfen muss, ob die Klausel, auf die sich die Universität berief, missbräuchlich im Sinne der Klausel-RL ist. Nach dem belgischen Verfahrensrecht muss ein Gericht, wenn der Beklagte nicht erscheint, nur prüfen, ob dem klägerischen Begehren zwingendes Recht entgegensteht, anderenfalls wird der Klage stattgegeben.

Der EuGH entschied, dass selbst bei einer Säumnis des Beklagten die Klausel, auf die der Kläger seinen Anspruch stützt, einer Überprüfung unterzogen werden muss. Der EuGH begründete dies mit dem Grundsatz der Äquivalenz, demnach ein Mitgliedstaat unionsrechtliche Sachverhalte nicht ungünstiger behandeln darf als innerstaatliche Sachverhalte. Wenn also das belgische Gericht zwingendes innerstaatliches Recht berücksichtigt, müsse es in gleicher Weise auch zwingendes Unionsrecht berücksichtigen. Zu diesem zwingenden Unionsrecht zähle die Klausel-RL.

Nachdem der EuGH dies geklärt hatte, stand noch die Antwort auf die Frage aus, ob der Anwendungsbereich der Klausel-RL im vorliegenden Fall überhaupt eröffnet war. Dafür müsste die Universität nämlich als Gewerbetreibende zu qualifizieren sein. Dem wurde entgegen gehalten, dass die Universität eine öffentlich-rechtliche Bildungseinrichtung ist, die mit ihrem Lehrauftrag Aufgaben im Allgemeininteresse erfüllt. Nach dem traditionellen Verständnis steht einer Eigenschaft als Gewerbetreibender auch entgegen, dass die Universität das Darlehen ohne Gewinnerzielungsabsicht und unentgeltlich vergab.

Nach dem EuGH sei dies jedoch unerheblich. Zunächst sei der öffentlich-rechtliche Charakter der Universität nach dem klaren Wortlaut der Klausel-RL unerheblich (Art. 2 lit. c Klausel-RL). Hinsichtlich der Eigenschaft als Gewerbetreibender sei auch nicht auf die allgemeine Lehrtätigkeit abzustellen. Es sei vielmehr auf den Zweck abzustellen, der mit dem jeweiligen Vertrag, hier also dem Darlehensvertrag verfolgt wird. Darüber hinaus spreche der Schutzzweck der Klausel-RL dafür, dass die fehlende Gewinnerzielungsabsicht und die Unentgeltlichkeit des Darlehensvertrages unerheblich seien. Die Richtlinie bezwecke, das gestörte Vertragsverhältnis zwischen einem Gewerbetreibenden und einem Verbraucher auszugleichen. Das Vertragsverhältnis sei gestört, weil ein Verbraucher gegenüber einem Gewerbetreibenden über eine schwächere Verhandlungsposition und einen geringeren Informationsstand verfüge. Zudem gehe mit dem Kostenrisiko, das mit einem gerichtlichen Verfahren verbunden ist, ein Abschreckungseffekt einher, der einen Verbraucher stärker treffe als einen Gewerbetreibenden. Dies begründe die Gefahr, dass der Verbraucher seine Rechte nicht wahrnimmt.

Mit diesen Gründen steht der EuGH für eine weite Auslegung des Begriffs des Gewerbetreibenden ein. Somit wird auch die Studentin im Ausgangsverfahren für schutzbedürftig erklärt, da sie sich als Verbraucherin mit der Universität einer Vertragspartei ausgesetzt sieht, die im Gegensatz zu ihr über eine starke Verhandlungsposition verfüge. Somit sei die Universität bei der Kreditvergabe an Studierende als Gewerbetreibende zu qualifizieren, auch wenn sie kein Gewerbe im traditionellen Sinne betreibt.

Der EuGH überließ es jedoch letztlich dem belgischen Gericht, zu bestimmen, ob die Klausel über die Zinsen und die Entschädigung tatsächlich missbräuchlich sei. Unionsrechtlich sei nur zwingend vorgegeben, dass in einer Situation wie im Ausgangsverfahren überhaupt eine Überprüfung der Klausel stattfindet.

III. Auswirkungen auf die Hochschulpraxis

Die erste Antwort des EuGH hat keine Bedeutung für die deutsche Hochschulpraxis. Denn was nun zum belgischen Verfahrensrecht entschieden wurde, entspricht bereits der deutschen Rechtslage. Erscheint in einem Prozess vor einem deutschen Gericht der Beklagte nicht, muss ohnehin geprüft werden, ob der Vortrag des Klägers schlüssig ist. Bei dieser Schlüssigkeitsprüfung würde ebenfalls geprüft, ob die Vereinbarung, auf die sich der Kläger beruft, wegen eines Verstoßes gegen Vorgaben der Klausel-RL unwirksam ist.

Von Bedeutung ist allerdings die Antwort auf die zweite Frage, mit der die Universität als Gewerbetreibender im Sinne der Klausel-RL qualifiziert wurde. Zwar kann der zugrundeliegende Sachverhalt aufgrund der weitgehenden Abschaffung der Studienbeiträge in Deutschland nicht als Beispiel dienen. Gleichwohl lässt sich die Entscheidung des EuGH auf vergleichbare Situationen übertragen. Denn einige Universitäten bieten weiterhin eigene Finanzierungsmöglichkeiten an, zum Beispiel über den Allgemeinen Studierendenausschuss (AStA). In diesen Fällen greift die Rechtsprechung des EuGH ebenso ein wie im belgischen Ausgangsfall.

Die Klausel-RL wurde durch die Bundesrepublik Deutschland in den §§ 305 ff. des Bürgerlichen Gesetzbuches (BGB) über die Kontrolle von Allgemeinen Geschäftsbedingungen (AGB) umgesetzt. Allgemeine Geschäftsbedingungen zwischen einem Verbraucher und einem Unternehmer sind alle vorformulierten Vertragsbedingungen, die eine Vertragspartei der anderen bei Abschluss eines Vertrags stellt. Die Vorschriften über die Allgemeinen Geschäftsbedingungen benutzen zwar den Begriff des Unternehmers statt den des Gewerbetreibenden. Der EuGH hat aber zum belgischen Recht, das ebenfalls den Begriff des Unternehmers verwendet, entschieden, dass dies keinen inhaltlichen Unterschied zur Folge habe.

Ein Unternehmer ist nach § 14 BGB jede Person oder rechtsfähige Personengesellschaft, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handelt. Bei der Auslegung dieses Unternehmerbegriffs muss also das Verständnis des EuGH im Wege

einer richtlinienkonformen Auslegung zugrunde gelegt werden. Folglich gelten die Vorgaben für Allgemeine Geschäftsbedingungen auch bei Darlehensverträgen zwischen Hochschulen und Studierenden. Hierbei ist beispielsweise zu berücksichtigen, dass von der Rechtsprechung aus dem Verbot einer unangemessenen Benachteiligung (§ 307 BGB) gefolgert wird, dass Klauseln zur Anpassung von Zinssätzen bei laufenden Darlehensverträgen nur unter strengen Voraussetzungen gültig sind. Ein anderes Beispiel für eine missbräuchliche Klausel findet sich in § 309 Nr. 3 BGB, wonach es unzulässig ist, dem Verbraucher zu verbieten, mit einer eigenen Forderung aufzurechnen.

Über die Klauselkontrolle hinaus findet sich der Begriff des Unternehmers auch in den Vorschriften über den Verbraucherdarlehensvertrag wieder. Auch der öffentlich-rechtliche Charakter einer Hochschule führt nicht dazu, dass diese aus dem Anwendungsbereich heraus fällt. Der Anwendungsbereich ist nur dann nicht eröffnet, wenn das Darlehen unter 200 Euro beträgt (§ 514 Abs. 1 S. 2, 491 Abs. 2 S. 2 Nr. 1 BGB). Somit ist die Hochschule als Darlehensgeber verpflichtet, die Kreditwürdigkeit des Verbrauchers zu prüfen (§§ 514 Abs. 1, 505a Abs. 1 S. 1 BGB) und über das Widerrufsrecht zu informieren (§ 514 Abs. 2 S. 3 BGB). Im Übrigen kann der Darlehensvertrag wegen Verzugs des Darlehensnehmers nur unter den erhöhten Anforderungen des §§ 514 Abs. 1 S. 1, 498 BGB gekündigt werden.

IV. Fazit

Aus dem Urteil des EuGH lassen sich folgende Schlussfolgerungen für die deutsche Hochschulpraxis ableiten. Für den Unternehmerbegriff des BGB spielt es keine Rolle, ob mit Gewinnerzielungsabsicht oder entgeltlich gehandelt wird. Auch Personen, die dem öffentlich-rechtlichen Bereich zuzurechnen sind, fallen nicht gleich aus dem Unternehmerbegriff heraus. Entscheidend ist nur, zu welchem Zweck der konkrete Vertrag geschlossen wird. Nach diesen Kriterien kann auch eine deutsche Hochschule Unternehmer sein und muss dann die verbraucherschützenden Vorschriften des BGB beachten.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de