DFN infobrief recht

7 / 2020
Juli 2020

Der Prüfling — Allein zu Haus

Zur datenschutzrechtlichen Rechtmäßigkeit von Maßnahmen im Zuge von Home-Klausuren

No news is better news

Fake News in Corona-Zeiten

Du kommst hier nicht rein!

Der Einsatz von Deauthentication-Paketen zur Abwehr von Rogue-Access-Points kann für Ärger mit der Bundesnetzagentur sorgen

Der Prüfling — Allein zu Haus

Zur datenschutzrechtlichen Rechtmäßigkeit von Maßnahmen im Zuge von Home-Klausuren

von Steffen Uphues

Als Folge der Corona-Pandemie erleben die öffentlichen Hochschulen zurzeit ein größtenteils digital gestaltetes Semester. Eine ganz besondere Herausforderung ist in diesem Zusammenhang die Gestaltung des Prüfungsablaufs. Je nach Bundesland bestehen Möglichkeiten, Präsenzprüfungen abzuhalten. Vielerorts wird es jedoch gerade in überlaufenen Studiengängen nicht möglich sein, in gewohntem Ablauf die Klausuren schreiben zu lassen. In diesem Zuge kam die Möglichkeit von Home-Klausuren auf die Liste alternativer Wahlmöglichkeiten. Dieser Beitrag soll nach einer kurzen Einführung der Frage nachgehen, ob die Anfertigung von Home-Klausuren und die damit einhergehende Überwachung der Prüflinge datenschutzrechtlich möglich ist.

I. Einführung

Unter dem Begriff der Home-Klausur im Sinne dieses Beitrags ist die Durchführung einer schriftlichen Prüfungssituation zu verstehen. Den Prüflingen steht ein begrenzter Zeitraum zur Verfügung und die Klausur soll ohne Hilfsmittel angefertigt werden. Dabei ist der prüfungsrechtliche Grundsatz der Chancengleichheit zu beachten. Dieser ergibt sich aus Art. 3 Grundgesetz (GG) und besagt, dass die Prüfung ermöglichen soll, den Wissensstand der einzelnen Studenten in einen Vergleich zu setzen. Mögliche Täuschungen über den wahren Wissensstand, etwa durch sogenannte Spickzettel oder Absprachen mit Kommilitonen während der Prüfungszeit, sollen ausgeschlossen werden. Im analogen Bereich erfolgt eine Kontrolle etwa durch: Abgabe von Smartphones bei der Aufsicht; Gänge von Aufsichtspersonen durch die Reihen, um etwaige Spickzettel ausfindig zu machen und Gespräche zwischen Studenten zu unterbinden; Kontrolle von Toilettengängen.

Um den prüfungsrechtlichen Gleichheitsgrundsatz auch im digitalen Bereich zu wahren, sind bestimmte Überwachungsmöglichkeiten der räumlichen Umgebung des Studenten im „Home Office“ denkbar. Ein prominentes Beispiel hierfür ist die Bucerius Law School in Hamburg. Dort soll es im Rahmen einer Home-Klausur dazu gekommen sein, dass noch während der Bearbeitungszeit eine Lösungsskizze der Klausur im Internet auftauchte. Die private Hochschule sah hierin einen Täuschungsversuch und ging dazu über, die Prüflinge per Video zu überwachen. Im Folgenden soll bewertet werden, ob ein solches Vorgehen auch für öffentliche Hochschulen eine gangbare Option darstellt. Hierfür sind zunächst die Maßnahmen in den Blick zu nehmen, die zur Überprüfung der Prüflinge angewendet werden können. Vor Beginn der Klausur ist eine Identifikationskontrolle durch die Aufsichtsperson via Videokonferenz durchzuführen. Ebenso sollte ein 360-Grad-Raumscan erfolgen. Hierdurch soll die Möglichkeit minimiert werden, dass Prüflinge auf an die Wand geheftete Notizen oder ähnliches zurückgreifen können. Während der Klausur kann eine Reihe von technischen Werkzeugen auf dem Rechner der Prüflinge genutzt werden. Diese können unterschiedlichen Zwecken dienen: Dem Verhindern eines zweiten Bildschirms; dem Schließen geöffneter Tabs und dem Unterbinden vom Öffnen neuer Tabs; der Deaktivierung der Zwischenablage; der zwingenden Anzeige im Vollbildmodus; der Deaktivierung der Druckfunktion. Daneben erfolgt während der Anfertigung der Klausur eine Video- und Audioüberwachung durch Aufsichtspersonen. Schnell wird klar: Im Rahmen von Home-Klausuren werden in erheblichem Umfang personenbezogene Daten verarbeitet. Durch die Maßnahmen erfolgt ein Eingriff in das Recht auf informationelle Selbstbestimmung der Prüflinge. Dieses Recht gewährt es jeder Person, selbst darüber zu bestim-

men, ob und in welchem Umfang sie ihre personenbezogenen Daten zugänglich machen möchte. Gerade durch eine Videoüberwachung verliert der Prüfling einiges an Privatsphäre. Viele Studenten haben nur ein Zimmer in einer Wohngemeinschaft. Dieses stellt ihren persönlichen Rückzugsort dar, von dem sie andere ausschließen können. Gerade diese Räumlichkeit muss nun im Rahmen einer Videoüberwachung anderen offenbart werden. Insofern stellt sich die Frage, inwiefern ein solcher Eingriff seitens der Hochschulen datenschutzrechtlich zu rechtfertigen ist.

II. Rechtmäßigkeit der Datenverarbeitungen im Rahmen von Home-Klausuren

Eine Verarbeitung personenbezogener Daten bedarf einer im Gesetz verankerten Erlaubnisgrundlage. Dieses Grundprinzip des Verbots mit Erlaubnisvorbehalt ist in Art. 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) normiert. Hiernach kommt für die Rechtfertigung einer Datenverarbeitung eine Einwilligung nach lit. a oder aber eine gesetzliche Erlaubnisgrundlage nach lit. b-f in Betracht. Für Datenverarbeitungen öffentlicher Hochschulen sind zwei mögliche Erlaubnisgrundlagen zu prüfen: Zum einen die Einwilligung nach lit. a und zum anderen die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe nach lit. e.

1. Datenverarbeitung aufgrund einer Einwilligung

Eine Datenverarbeitung ist nach Art. 6 Abs. 1 lit. a DSGVO rechtmäßig, wenn die betroffene Person im Vorfeld über die Zwecke der Datenverarbeitung informiert wurde und eingewilligt hat. Diese Einwilligung muss insbesondere freiwillig erteilt werden, wie Art. 4 Nr. 11 DSGVO unmissverständlich formuliert.

Dem Merkmal der Freiwilligkeit kommt im Verhältnis zwischen öffentlicher Hochschule und Student eine besondere Bedeutung zu. Erwägungsgrund 42 S. 5 DSGVO fordert für ein freiwilliges Handeln, dass die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. Speziell zum Machtgefälle zwischen öffentlichen Stellen und Bürgern äußert sich Erwägungsgrund 43 S. 1 DSGVO. Hiernach bestehe zwischen Behörde und Bürger ein derartiges Ungleichgewicht, dass grundsätzlich anzunehmen ist, eine Einwilligung könne nicht freiwillig abgegeben werden. Zwar können Prüflinge im Regelbetrieb ebenfalls nicht über die Bedingungen bestimmen, unter welchen sie ihre Prüfung ablegen. Auch bei Präsenzklausuren stehen sie durchgängig unter Aufsicht. Jedoch kommt es dort eben nicht zu einem Eingriff in die räumliche Privatsphäre.

In den meisten Fällen besteht die Möglichkeit, Home-Klausuren zu verweigern bzw. sich schlichtweg nicht zu diesen anzumelden. Sofern die Studenten die Prüfungsleistung erst zu einem späteren Zeitpunkt ablegen dürften, könnte dies ihren Studienabschluss verzögern. Insofern würde sich aus dem Verweigern der Einwilligung ein mittelbarer Nachteil für die Studenten ergeben. Mit Blick hierauf sind Präsenzklausuren als Alternative zu beachten. Für diejenigen, die keine Home-Klausur schreiben möchten, kann ein solches Präsenzangebot geschaffen werden. Besteht die Möglichkeit, die Prüfung unter Aufsicht und unter Einhaltung aller infektionsbedingten Sicherheitsmaßnahmen abzulegen, so ist dies den Studenten zuzumuten. Das Verweigern der Einwilligung würde die Studenten in diesem Fall aufgrund des Alternativangebots nicht benachteiligen.

Eine Rechtfertigung der Datenverarbeitung aufgrund einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erscheint nach den vorangegangenen Ausführungen unter Umständen möglich. Jedoch zeigen die angesprochenen Problemfelder, dass erhebliche Bedenken in datenschutzrechtlicher Hinsicht bestehen.

Sofern die Hochschule als Verantwortlicher der Datenverarbeitung auf eine Einwilligung zurückgreifen möchte, ist die Möglichkeit des Widerrufs nach Art. 7 Abs. 3 S. 1 DSGVO zu beachten. Hiernach kann eine betroffene Person die von ihr erteilte Einwilligung jederzeit widerrufen. Eine bis dahin erfolgte Datenverarbeitung bleibt in ihrer Rechtmäßigkeit zwar unberührt. Jedoch ist die Datenverarbeitung im Fortlauf nicht mehr durch die Einwilligung gerechtfertigt. Daneben besteht nach Art. 17 Abs. 1 lit. b DSGVO für die betroffene Person das Recht, den Verantwortlichen zur Löschung der personenbezogenen Daten zu veranlassen, sofern diesem keine anderweitige Erlaubnisgrundlage zur Verfügung steht. Dies steht im Widerspruch zu der Dokumentationspflicht der Hochschulen, die im Rahmen von Prüfungsleistungen besteht. Der Grundsatz des effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG erfordert, dass

einem Prüfling die behördliche und gerichtliche Überprüfung der Bewertung einer von ihm erbrachten Prüfungsleistung zusteht. Insofern sind die Hochschulen bis zu einem gewissen Grad und einer gewissen Zeit verpflichtet, die Dokumentation des Prüfungsablaufs aufzubewahren. Ein Widerspruch zum Recht auf Löschung nach Art. 17 Abs. 1 lit. b DSGVO entsteht hierdurch jedoch nicht. Denn in Art. 17 Abs. 3 lit. b DSGVO ist normiert, dass die Löschpflicht aus Abs. 1 für den Verantwortlichen nicht besteht, soweit die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung erfolgt. Die in den Prüfungsordnungen festgelegten Dokumentationspflichten dürften als eine solche rechtliche Verpflichtung einzuordnen sein.

2. Datenverarbeitung aufgrund gesetzlicher Erlaubnisgrundlagen

Als weitere Erlaubnisgrundlage für die Datenverarbeitung kommt Art. 6 Abs. 1 lit. e DSGVO in Betracht. Hiernach ist eine Datenverarbeitung gerechtfertigt, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Es handelt sich bei lit. e um eine sogenannte Scharniernorm. Die Norm selbst bietet also nicht unmittelbar die Rechtsgrundlage für eine Datenverarbeitung. Es muss vielmehr eine gesondert normierte Rechtsgrundlage bestehen, die die Aufgabenwahrnehmung näher ausgestaltet. Diese Rechtsgrundlage kann nach Art. 6 Abs. 3 DSGVO durch Unionsrecht, aber auch durch das Recht der einzelnen Mitgliedstaaten geschaffen werden.

Hieraus ergibt sich, dass die nationalen Gesetzgeber in Deutschland eigenständig Regelungen für öffentliche Stellen wie etwa Hochschulen erlassen können. In diesem Zusammenhang sind insbesondere die landesrechtlichen Datenschutz- und Hochschulgesetze maßgeblich. Insofern ist es wichtig, dass sich jede Hochschule an den für sie geltenden landesrechtlichen Regelungen orientiert. Als Ausprägung des föderalistischen Systems können sich deutschlandweit erhebliche Unterschiede in der rechtlichen Bewertung ergeben. Dieser Beitrag kann somit keine pauschale Antwort liefern, ob öffentlichen Hochschulen eine taugliche Rechtsgrundlage im Sinne von Art. 6 Abs. 1 lit. e DSGVO zur Verfügung steht. Zwei Beispiele können jedoch dabei helfen, die Auswirkungen der unterschiedlichen Regelungen zu verdeutlichen:

In § 17 Abs. 1 S. 1 des Niedersächsischen Hochschulgesetzes (NHG) ist normiert, dass Hochschulen personenbezogene Daten von Studenten unter anderem dann verarbeiten dürfen, wenn diese Datenverarbeitung für die Teilnahme an Prüfungen erforderlich ist und entsprechende Hochschulordnungen hierzu existieren. Die Datenverarbeitung im Rahmen von Home-Klausuren könnte hiernach über die Scharniernorm des Art. 6 Abs. 1 lit. e DSGVO gerechtfertigt sein.

In Nordrhein-Westfalen besteht keine vergleichbare Regelung. § 8 Abs. 5 des Hochschulgesetzes NRW (HG NRW) äußert sich lediglich allgemein dahingehend, dass die Verarbeitung personenbezogener Daten unter Beachtung der allgemeinen datenschutzrechtlichen Vorschriften stattfindet. Mitunter wird vertreten, dass Hochschulen sich mit Blick auf Datenverarbeitungen auf die allgemeine Aufgabenzuweisung nach §§ 58 ff. HG NRW berufen können. Diese Normen äußern sich jedoch nicht konkret genug zu möglichen Datenverarbeitungen und den zugrundeliegenden Zwecken. Insofern dürfte – nach jetzigem Stand – in Nordrhein-Westfalen keine Rechtfertigung über Art. 6 Abs. 1 lit. e DSGVO möglich sein.

III. Fazit für öffentliche Hochschulen

Auch in der momentanen Ausnahmesituation haben die Hochschulen das Datenschutzrecht zu beachten und die dort normierten Grundsätze und Regelungen zu wahren. Im Umgang mit der Privatsphäre der Studenten ist eine gesteigerte Sensibilität erforderlich. Dies gilt mit Blick auf eine Einwilligung gerade hinsichtlich der Freiwilligkeit – etwaige Nachteile im Falle einer Verweigerung sollten minimiert werden. Die Möglichkeit des Widerrufs stellt für die Datenverarbeitung dagegen keine Risiken dar. Zwar resultiert hieraus grundsätzlich ein Recht auf Löschung der personenbezogenen Daten. Die Hochschulen dürfen die Daten jedoch solange aufbewahren wie es zur Ermöglichung von Überprüfungsansprüchen seitens der Prüflinge erforderlich ist.

Bei der Frage, ob eine gesetzliche Erlaubnisgrundlage über Art. 6 Abs. 1 lit. e DSGVO heranzuziehen ist, muss stets das jeweilige Landesrecht beachtet werden. Wenn eine Datenverarbeitung im Rahmen von Prüfungen nicht in die Regelungen mitaufgenommen wurde, liegt im Zweifel keine hinreichend konkrete Anknüpfungsnorm vor.

Anders als für öffentliche Hochschulen bieten sich für pri-

vate Hochschulen noch weitere mögliche Erlaubnisgrundlagen. So kommen im Verhältnis einer privaten Hochschule zu ihren Studierenden auch eine Datenverarbeitung aufgrund vertraglicher Verpflichtungen nach Art. 6 Abs. 1 lit. b DSGVO sowie berechtigte Interessen der Hochschulen nach Art. 6 Abs. 1 lit. f DSGVO in Betracht.

No news is better news

Fake News in Corona-Zeiten

von Marten Tiessen

In einem offenen Brief appellierten Ärzte und Gesundheitsexperten aus der ganzen Welt an die großen sozialen Netzwerke, stärker gegen falsche Berichterstattung vorzugehen. Das schon länger virulente Problem der „Fake News“ scheint in Corona-Zeiten ein neues Ausmaß erreicht zu haben. Gerade im Gesundheitsbereich können, begünstigt durch die Ängste der Bevölkerung, Fake News verheerende Folgen haben. Wissenschaftseinrichtungen, die der Flut von falschen Informationen belegbare Forschung entgegensetzen, haben keinen leichten Stand. Auch rechtlich scheint sich das Problem nicht ohne Weiteres lösen zu lassen.

I. Gefahr durch Fake News

„Fake News“ ist ein ambivalenter Begriff. Er verdeutlicht auf verschiedene Weise das Problem der schwindenden Glaubwürdigkeit medialer Berichterstatter. Zum einen beschreibt er das sehr reale Phänomen zielgerichteter Desinformation, vor allem verbreitet über soziale Netzwerke. Zum anderen wird er zunehmend als Kampfbegriff gegenüber unliebsamer politischer Berichterstattung verwendet. Dabei soll durch den Begriff jede inhaltliche Auseinandersetzung von vornherein vermieden werden, indem Nachrichten als pauschal wahrheitswidrig abgekanzelt werden. In beiden Fällen unterscheidet sich nur die Verwendung, nicht hingegen die Bedeutung des Begriffs. Übersetzen lässt sich „Fake News“ am besten mit bewusster Falschmeldung (Falschnachrichten). Im Gegensatz zu einer irrtümlichen Falschmeldung geht es bei Fake News vielmehr um gezielte Desinformation. Sie dient der politischen Agitation, geschäftlichen Interessen oder schlicht dem Drang nach Aufmerksamkeit.

Vermehrten Gebrauch erfuhr der Begriff erstmals im Zusammenhang mit dem US-Wahlkampf 2016. Seitdem ist kaum ein Tag vergangen, an dem der amerikanische Präsident den Begriff nicht verwendet hat. Seine Versuche kritische Medien und politische Gegner als Lügner zu desavouieren, stehen dabei im starken Widerspruch zu seinem eigenen Umgang mit der Wahrheit. Sein Lieblingsmedium Twitter nutzt er zur Verbreitung von Verschwörungstheorien und anderen Unwahrheiten. Bislang hatte Twitter das Verhalten seines bekanntesten Nutzers geduldet. Jetzt wurde einer seiner Tweets zum ersten Mal mit einem Hinweis zu gegenüberstellenden Informationen versehen. Twitter begründete den nicht unumstrittenen Eingriff mit der Änderung seiner Richtlinien. Angesichts der Flut von Falschinformationen bezüglich des Corona-Virus‘ sah Twitter sich erst kürzlich veranlasst, seine Position als passive Plattform aufzugeben. Das steht im Einklang mit anderen sozialen Medien, die seit der Corona-Krise anfangen, ihren Umgang mit irreführenden Informationen zu überdenken.

Mit der Pandemie hat das Fake News-Problem ein neues Ausmaß erreicht: Teilweise wird schon von einer sogenannten Infodemie gesprochen. Selbst das Bundesgesundheitsministerium warnte vor gefährlichen Falschnachrichten. Immerhin sieben Prozent aller Posts in sozialen Netzwerken zum Thema Corona-Virus enthalten nach Einschätzungen des Europäischen Auswärtigen Dienstes Desinformationen. Problematischer als die Menge sind jedoch die Inhalte selbst. Dabei ist der Strauß an Falschnachrichten äußerst bunt: Sie betreffen Ursache, Ausbreitung, Symptome, Risikogruppen, staatliche Maßnahmen und mögliche Heilmittel. Über all diese Themen kursieren Fehlinformationen im Netz, die nicht nur für Unsicherheit sorgen, sondern auch gefährlich sein können. Gerade die Empfehlung vermeintlicher Wundermittel gegen das Virus kann schwerwiegende gesundheitliche Folgen haben.

Das Gefährdungspotential von Falschmeldungen verändert sich zudem mit der Verbreitungsart. Falschmeldungen hat es in der einen oder anderen Form schon immer gegeben. Neu sind hingegen die technischen Möglichkeiten der Berichterstattung. Große Teile der Gesellschaft beziehen inzwischen ihre Nachrichten nicht mehr über traditionelle Print-Medien oder das Fernsehen, sondern über soziale Netzwerke. Die sozialen Netzwerke schalten dabei nicht selbst Anzeigen oder schreiben Artikel, sondern ermöglichen anderen Nutzern oder Drittanbietern, Artikel zu posten. Die Leistung der Netzwerke besteht darin, Algorithmen zu entwickeln, die vorgeben, wem welcher Artikel angezeigt wird. Je mehr sich ein Nutzer für einen Artikel interessiert, desto häufiger werden ihm ähnliche Artikel angezeigt. Das kann dazu führen, dass ein Nutzer seine Nachrichten nur noch von einer oder wenigen Quellen bezieht. Er lebt dann in der sogenannten Filterblase. In dieser Blase sind die Meinungsbildung und die Wahrnehmung der Betroffenen sehr leicht beeinflussbar, weil es an widersprechenden Quellen fehlt. Dementsprechend können Fehlinformationen eine unheilvollere Wirkung entfalten.

II. Rechtliches Vorgehen gegen Fake News

Falsche Tatsachenbehauptungen werden nicht durch die Meinungsfreiheit nach Art. 5 Abs. 1 GG geschützt. Der fehlende Schutz führt aber nicht automatisch zur Rechtswidrigkeit der Aussage. Regelungen, die Fake News aufgrund ihres irreführenden Inhalts pauschal verbieten oder sanktionieren, gibt es im deutschen Recht nicht. Zwar kennt das Strafrecht durchaus Straftatbestände, die durch das Verbreiten von Fake News erfüllt sein können. Ob die Voraussetzungen dafür jedoch im Einzelfall vorliegen, hängt stark von dem Inhalt der Meldung ab.

Werden über eine bestimmte Person, wie zum Beispiel den politischen Gegner, falsche Tatsachenbehauptungen aufgestellt, kommt vor allem eine Strafbarkeit wegen Verleumdung nach § 187 StGB oder übler Nachrede nach § 186 StGB in Betracht. Beide Straftaten setzen voraus, dass die verbreitete Tatsache geeignet ist, den Betroffenen verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen. Bei einer Verleumdung erfolgt die Behauptung wider besseres Wissen, während für eine üble Nachrede bereits ausreichend ist, dass die Tatsache nicht erweislich wahr ist. Den Nachweis, dass die Aussage wahr ist, muss dabei derjenige erbringen, der sie geäußert hat. Wie auch bei der Beleidigung kann aber die Wahrnehmung berechtigter Interessen gemäß § 193 StGB den Täter entlasten. Verfolgt werden beide Delikte nur, sofern ein Antrag des Geschädigten vorliegt.

Unter Umständen könnte die Verbreitung von Fake News auch den Tatbestand der Volksverhetzung nach § 130 Abs. 2 Nr. 2 StGB erfüllen, sofern eine neutrale aber bewusst falsche Behauptung den Hass gegen Teile der Bevölkerung anstachelt. Die Hürden für die Erfüllung des Deliktes dürften allerdings recht hoch sein. Eindeutig lässt sich eine Strafbarkeit wegen Volksverhetzung bei Verbreitung der sogenannten Auschwitz-Lüge nach § 130 Abs. 3 StGB feststellen (vgl. BGH, Urteil vom 12. 12.2000 - 1 StR 184/00). Einen so eindeutigen Tabubruch enthalten Fake News bezüglich Corona indes nicht.

In Extremfällen, in denen es zu Gesundheitsschädigungen aufgrund von Falschinformation kommt, wäre eine Strafbarkeit wegen Körperverletzungsdelikten in mittelbarer Täterschaft zu prüfen. Ob die Bedingungen dafür erfüllt sind und insbesondere ein Tatvorsatz nachgewiesen werden kann, ist allerdings fraglich. Ein solcher Fall wurde bisher noch nicht gerichtlich entschieden.

Zivilrechtlich kann über §§ 823 Abs. 1, 823 Abs. 2 BGB oder die analoge Anwendung von § 1004 BGB gegen Persönlichkeitsrechtsverletzungen vorgegangen werden. Hiernach steht dem Verletzten ein Anspruch auf Widerruf oder Richtigstellung zu. Damit der Verletzte überhaupt die Identität des Täters ermitteln und Ansprüche gegen ihn geltend machen kann, steht ihm gegenüber dem sozialen Netzwerk ein Auskunftsanspruch aus § 14 Abs. 3 TMG zu. Danach sind Diensteanbieter verpflichtet, Bestandsdaten herauszugeben, die zur Durchsetzung zivilrechtlicher Ansprüche erforderlich sind.

Bisher gibt es in Deutschland erst wenige Gerichtsentscheidungen, die sich mit der Verbreitung von Fake News auseinandergesetzt haben. Das AG Mannheim (Urteil vom 7.1.2019 – 20 Cs 806 Js 10181/18) verurteilte im letzten Jahr einen Mann wegen Störung des öffentlichen Friedens durch Androhung von Straftaten gem. § 126 StGB. Als Betreiber des „Rheinneckarblogs“ hatte er einen erfundenen Text gepostet, indem von „50 Angreifern“ die Rede war, die in Mannheim „für ein Blutbad apokalyptischen Ausmaßes“ verantwortlich seien. Aus dem Artikel entstand zunächst der Eindruck, die Täter seien noch auf freiem Fuß und würden ihre Attacken in der

Innenstadt fortsetzen. Erst nach Abschluss eines Abonnement-Vertrags war der hinter einer Paywall liegende Artikel ganz einsehbar und erkennbar, dass es sich um ein fiktives Geschehnis handelte. Das Gericht war der Ansicht, dass durch den Artikel im Sinne von § 126 Abs. 2 StGB vorgetäuscht wurde, dass die Verwirklichung eines Mordes, Totschlags oder einer schweren Körperverletzung bevorstehe.

Solche exotischen Fälle repräsentieren nur einen Bruchteil der Falschnachrichten. Bei Falschmeldungen im Zusammenhang mit Corona werden die Voraussetzungen für ehrverletzende Delikte oder zivilrechtliche Berichtigungsansprüche häufig nicht vorliegen, da die Nachricht keine Aussage über Einzelpersonen enthält. Fehlt die persönliche Betroffenheit oder besteht kein strafbewehrtes Sprechverbot, lässt sich weder strafrechtlich noch zivilrechtlich gegen Fake News vorgehen.

III. Das NetzDG und die Störerhaftung

Das Netzwerkdurchsetzungsgesetz (NetzDG), das als vermeintliches Mittel gegen Hass im Netz in aller Munde war, bietet keine neuen Anspruchsgrundlagen, sondern regelt hauptsächlich die Löschfristen der Plattformbetreiber beim Vorliegen von bestimmten Straftaten. Diese sind in § 1 Abs. 3 NetzDG abschließend aufgelistet. Zu ihnen gehören die genannten Straftatbestände aus §§ 130, 186, 187 und 126 StGB.

Plattformbetreiber sind zwar als Störer verpflichtet, strafbare Inhalte von der Plattform zu entfernen. Ihre Verantwortung wird aber durch die Privilegierung aus § 10 Telemediengesetz (TMG) erheblich eingeschränkt. Sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Fall von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, sind Diensteanbieter nicht für fremde Informationen verantwortlich. Da sie aber nicht verpflichtet sind, von sich aus alle Inhalte auf ihre Rechtmäßigkeit zu überprüfen, erlangen Plattformen in der Regel erst Kenntnis, wenn der Betroffene eine Beschwerde einlegt. Anders als beim Strafantrag kann die Beschwerde nicht nur vom Verletzten, sondern von jedem Nutzer eingelegt werden. Die Beschwerde muss wiederum hinreichend substantiiert und konkret sein. Eine Verpflichtung der Plattformbetreiber, den Wahrheitsgehalt durch einen Faktencheck selbst zu überprüfen, besteht nicht. Auch Sorgfaltspflichten, wie sie für Rundfunkveranstalter nach § 10 Rundfunkstaatsvertrag (RStV) bestehen, kennt das NetzDG nicht. Ist die Rechtswidrigkeit nicht offensichtlich oder liegt nicht bereits ein abgeschlossenes Strafverfahren vor, sind die Diensteanbieter daher nicht zum Handeln verpflichtet. Immerhin verpflichtet § 3 Abs. 2 Nr. 1 NetzDG die Plattformbetreiber zum unverzüglichen Bearbeiten der Beschwerden.

Nach der Gesetzesbegründung des NetzDG sollen die Regelungen ausdrücklich der Bekämpfung von Fake News dienen. Diesem Ziel wird das NetzDG nur bedingt gerecht. Indem das Gesetz nur die Rechtsdurchsetzung regelt und keine neuen Ansprüche schafft, fallen ein Großteil der Fake News gar nicht in den Anwendungsbereich des NetzDG.

IV. Alternative Maßnahmen und Ausblick

Letztlich fehlt es (noch) an geeigneten juristischen Mitteln, um Fake News den Riegel vorzuschieben. Ob solche Regelungen noch erlassen werden und welchen Inhalt sie hätten, ist zurzeit noch nicht absehbar. Wie unlängst Niedersachsens Innenminister Boris Pistorius, fordern manche, dass Falschnachrichten mit Bußgeldern oder Strafandrohung bewehrt werden. In anderen Ländern ist man schon einen Schritt weiter oder vielleicht zu weit gegangen. Vorhaben in anderen Ländern, wie Italien, Russland, Singapur oder Nigeria, Sanktionsgesetze gegen Fake News zu erlassen, ernteten heftige Kritik. Sie wurden als massive Einschnitte in die Meinungs- und Pressefreiheit bewertet und laufen Gefahr, einer staatlichen Zensur gleichzukommen. Auch Hessen, Bayern und Sachsen-Anhalt brachten eine Gesetzesinitiative auf den Weg, die wenig positive Resonanz fand und letztlich abgelehnt wurde.

Viele Politiker in Deutschland sprechen sich ausdrücklich gegen eine Ausweitung des Strafrechts aus und setzen sich stattdessen für eine bessere Aufklärung ein. Denn das beste Mittel gegen Fake News scheint bislang seriöse Berichterstattung aus vertrauenswürdigen Quellen zu sein. Damit in der Pluralität der Nachrichtenkanäle wichtige Informationen nicht untergehen, sollten deshalb gerade auch Hochschulen und Forschungseinrichtungen darauf bedacht sein, im Getöse um Corona eine kräftige Stimme zu beweisen. Mit fundierten wissenschaftlichen Erkenntnissen können sie Verschwörungstheorien widerlegen, Halbwahrheiten komplementieren und die nötige Rationalität in emotionale gesellschaftliche Themen bringen.

Soll die Verbreitung von Fake News direkt an der Wurzel gestoppt werden, steht es den Plattformen frei, selbst aktiv

zu werden. Bei Inhalten mit Corona-Bezug haben die sozialen Netzwerke schon freiwillig reagiert. YouTube priorisiert amtliche oder seriöse Videos und zeigt sie weiter dem User in der Ansicht weiter oben an. Zudem werden Videos, die Corona betreffen, mit einem Hinweis auf weiterführende Informationen versehen. Als gefährlich ansgesehene Videos werden von YouTube teilweise ganz gelöscht. Außerdem ist die Monetarisierung in diesen Fällen ausgeschaltet. Das bedeutet, dass vor den Videos keine Werbung mehr angezeigt wird und mit Corona-Inhalten somit kein Geld gemacht werden kann. Eine ähnliche Priorisierung nach Seriosität wie YouTube nimmt auch Instagram vor. WhatsApp kann aufgrund der Verschlüsselung gefährliche Nachrichten nicht filtern, schränkt aber die Weiterleitung von Nachrichten ein. Wie im Fall des amerikanischen Präsidenten versieht Twitter Falschnachrichten mit einem Link zu einem Faktencheck. Die Plattform versucht so gerade der Verbreitung von Verschwörungstheorien entgegenzuwirken. Enthält ein Post beispielswese das Wort „Corona" und „5G", versieht Twitter den Beitrag mit einem Link „zu den Fakten über COVID-19". Folgt er dem Link, erhält der Nutzer zahlreiche Beiträge, welche die Theorie, das 5G-Netz verursache das Virus, widerlegen. In Einzelfällen löscht Twitter irreführende Beiträge, wenn sie die öffentliche Sicherheit gefährden oder ernsthafte Schäden verursachen können. Auch Facebook löscht Einträge, wenn sie gesundheitsgefährdende Behauptungen enthalten. Inhalte, die sich nach einem Faktencheck zwar als irreführend herausstellen, aber keine direkte Gefahr für die Gesundheit darstellen, versieht Facebook dagegen mit einem Warnhinweis. Allerdings dauert die Überprüfung der Inhalte und die Hinweise werden teilweise erst nach Tagen angezeigt. Bis dahin können die Inhalte aber schon eine große Reichweite erlangen. Der Faktencheck, den Facebook durch das Recherche-Netzwerk Correctiv vornehmen lässt, war kürzlich Gegenstand einer gerichtlichen Auseinandersetzung (OLG Karlsruhe, Urteil vom 27.05.2020 - 6 U 36/20). Die im Eilverfahren getroffene Entscheidung betraf allerdings nicht die Rechtmäßigkeit des Faktenchecks insgesamt, sondern prüfte, ob es im konkreten Fall durch eine missverständliche Faktenprüfung zu einem Wettbewerbsverstoß kam. Irreführende Posts von Politikern schränkt Facebook anders als Twitter bislang nicht ein, da hier nach eigenen Aussagen das Interesse der Öffentlichkeit an der Aussage größer und ein Eingriff in die Meinungsbildung durch das Unternehmen bedenklicher sei. Gerade hierfür wurde Facebook zuletzt sogar aus den eigenen Reihen kritisiert.

Dabei sind die Bedenken Facebooks sicherlich nicht pauschal von der Hand zu weisen. Obwohl Plattformen als „cheapest cost avoider" die einfachste Möglichkeit haben, die Verbreitung von Fake News einzuschränken, bestehen bei ihrem Vorgehen – wenngleich in abgeschwächter Form – ähnliche Bedenken, wie bei staatlichen Verboten. Werden außerdem nur zu ausgewählten Themen Faktenchecks durchgeführt, kann dies für den Nutzer irreführend sein. Er geht unter Umständen davon aus, dass alle Nachrichten ohne Warnhinweis im Umkehrschluss die Faktenprüfung bestanden haben. Es bleibt abzuwarten, wie effektiv die aktuellen Maßnahmen sind. Ein goldener Weg im Umgang mit Fake News hat sich offenbar noch nicht etabliert.

Zu vorschnell sollte man bei der Einstufung von Nachrichten als Fake News übrigens nicht sein. Der Vorwurf „Fake News" zu verbreiten ist nach Ansicht des LG Hamburgs (Urteil vom 3.11.2017 – 324 O 219/17) eine Tatsachenbehauptung, die sich vollumfänglich gerichtlich überprüfen lässt. Sofern die Wahrheit der Behauptung nicht nachgewiesen wird, kann der Vorwurf eine Persönlichkeitsrechtsverletzung darstellen. Der Begriff sollte also nicht leichtfertig öffentlich verwendet werden.

Du kommst hier nicht rein!

Der Einsatz von Deauthentication-Paketen zur Abwehr von Rogue-Access-Points kann für Ärger mit der Bundesnetzagentur sorgen

von Owen Mc Grath

Zur einfachen und effizienten Abwehr von Rogue-Access-Points werden immer wieder sogenannte Deauthentication-Pakete (Deauth-Pakete, auch: WLAN-Deauther) eingesetzt. Durch Aussenden dieser Pakete wird ein Verbindungsaufbau mit solchen Netzwerkzugängen mit Schädigungsabsicht unterbunden. Die Bundesnetzagentur (BNetzA) hat den Einsatz von WLAN-Deauthern bereits wiederholt als Verstoß gegen Allgemeinzuteilungen eingestuft.

I. Der Einsatz von Deauth-Paketen

Mit dem Ziel, Nutzungs- und Zugangsdaten auszulesen, werden in Reichweite von öffentlichen WLAN-Zugän-gen immer wieder sogenannte Rogue-Access-Points errichtet. Diese Netzwerkzugänge kopieren beispielsweise die SSID (Netzwerkkennung) von öffentlichen Netzwerken und veranlassen Nutzer hierdurch sich in das von ihnen eingerichtete Netzwerk einzuwählen. Unter der Vorspiegelung ordnungsgemäßer Nutzungsmöglichkeit werden so Daten zum Nachteil der Nutzer ausgelesen. Auch an mehreren Hochschulen ist es in letzter Zeit zu Problemen mit fremden Netzwerkzugängen gekommen. Diese spiegeln dann zumeist die Nutzerkennung des Uni-Netzwerks. Zur Bekämpfung dieser unautorisierten Access-Points setzen Hochschulen und Forschungseinrichtungen zum Teil Deauth-Pakete ein. Durch Aussenden dieser Pakete wird der Verbindungsaufbau zwischen den Nutzern und den fremden Zugangspunkten unterbrochen. Allerdings können Deauth-Pakete auch Verbindungen zu Netzwerkzugängen ohne Schädigungsabsicht unterbinden, sofern die Pakete nicht zielgerichtet eingesetzt werden.

Die Bundesnetzagentur hat bereits einige Institutionen wegen des Einsatzes von Deauth-Paketen abgemahnt. Hierin liege ein Verstoß gegen Allgemeinzuteilungen der BNetzA. Fraglich ist, wie diese Allgemeinzuteilungen rechtlich einzuordnen sind.

II. Abmahnungen der BNetzA auf Grundlage von Allgemeinzuteilungen

In ihrer Abmahnung und ebenso auf Nachfrage, vermutlich einer Hochschule, rügt die BNetzA den Verstoß von WLAN-Deauthern gegen die Verfügung 10/2013 (geändert mit Verfügung 64/2018) und die Verfügung 7/2010 (geändert mit Verfügung 65/2018 und Verfügung 151/2018). Nach beiden Verfügungen dürfen „bestimmungsgemäße WLAN-Nutzungen“ nicht gestört werden.

Bei der BNetzA handelt es sich um eine Bundesoberbehörde. Einzustufen sind die relevanten Allgemeinzuteilungen demnach als konkret-generelle Verwaltungsakte und mithin als Allgemeinverfügungen nach § 35 S. 2 Verwaltungsverfahrensgesetz (VwVfG).

Verwaltungsakte sind von Behörden erlassene Regelungen mit unmittelbarer Außenwirkung, die auf eine Rechtsfolge gerichtet sind. Durch das Element der Außenwirkung wird festgelegt, dass nicht bloß ein behördeninterner Sachverhalt geregelt wird, sondern gerade externe Adressaten betroffen sind.
Grundsätzlich sind Verwaltungsakte konkret-individuelle Regelungen, welche sich an einen einzelnen Adressaten richten. Betrifft die Regelung allerdings einen bestimmten oder bestimmbaren weiteren Kreis an Adressaten liegt ein konkret-genereller Verwaltungsakt und mithin eine Allgemeinverfügung vor.

In Abgrenzung zu Rechtsnormen haben Verwaltungsakte – also auch Allgemeinverfügungen – einen konkreten Inhalt. Rechtsnormen hingegen regeln Sachverhalte abstrakt und bedürfen für die spezifische Anwendung im Einzelfall näherer Auseinandersetzung. Aber genau wie Rechtsnormen sind auch Verwaltungsakte auf eine Rechtsfolge gerichtet und entfalten Verbindlichkeit gegenüber dem Einzelnen. Bei Missachtung der behördlich gesetzten Regelungen ist mit Konsequenzen in Form von Zwangsmaßnahmen oder Bußgeldern zu rechnen.
Bestehen Bedenken gegenüber den durch eine Behörde in Form eines Verwaltungsaktes bzw. einer Allgemeinverfügung getroffenen Regelungen, können diese angegriffen werden. Die Rechtsmittel, die zur Verfügung stehen, sind ggf. ein Widerspruch und der Klageweg. Für beide Alternativen ist jedoch die entsprechende Frist zu wahren. Um Rechtssicherheit zu schaffen, haben auch möglicherweise rechtswidrige Verwaltungsakte, welche nicht in der Rechtsmittelfrist angegriffen wurden, Bestandskraft. Tatsächlich unwirksam werden sie erst dann, wenn sie nichtig nach § 44 VwVfG sind. Nichtigkeit eines Verwaltungsaktes ist allerdings eine seltene Ausnahme. Im weiteren Ausnahmefall kann auch das Wiederaufgreifen des Verfahrens nach § 51 VwVfG beantragt werden. Ferner können Verwaltungsakte mit Bestandskraft, rechtwidrig oder nicht, einseitig durch die erlassende Behörde wieder zurückgenommen werden (§§ 48, 49 VwVfG).
Auch wenn die Bestandskraft eines möglicherweise rechtswidrigen Verwaltungsaktes für den Laien widersprüchlich erscheinen mag, so ist sie dennoch eine grundgesetzlich gesicherte Notwendigkeit aus Gründen der Rechtssicherheit.

III. Behandlung der Allgemeinverfügungen

Die Abmahnungen, die die BNetzA aufgrund des Einsatzes von Deauth-Paketen gegen Netzwerkzugänge mit Schädigungsabsicht ausgesprochen hat, stoßen auf Unverständnis. Das Aussenden der Pakete ist eine effiziente und einfach zu implementierende Abwehrmöglichkeit gegen Rogue-Access-Points. Andere Maßnahmen, wie das Aufspüren und manuelle Entfernen der Hardware, von welcher die Störung ausgeht, stellen sich als sehr umständlich und wenig erfolgversprechend dar.
Um diesen Bedenken Rechnung zu tragen ist zu klären, ob der Einsatz von Deauth-Paketen tatsächlich gegen die Allgemeinverfügungen der BNetzA verstößt, wie gegen diese Allgemeinverfügungen vorzugehen ist und welche Konsequenzen ein Verstoß mit sich bringt.

Die Allgemeinzuteilungen der BNetzA verbieten eine Störung von „bestimmungsgemäße[n] WLAN-Nutzungen". Das Aussenden von Deauth-Paketen ist jedenfalls eine Störung der WLAN-Nutzung.
Fraglich ist allerdings, wann eine tatsächlich bestimmungsgemäße WLAN-Nutzung gestört ist. Der Betrieb eines Rogue-Access-Points geschieht in erster Linie mit Schädigungsabsicht. Eine solche Benutzung stellt wohl gerade eine bestimmungswidrige WLAN-Nutzung dar. Nur eine bestimmungsgemäße Nutzung ist im Rahmen der Allgemeinverfügungen geschützt. Dass es sich bei Rogue-Access-Points, entsprechend der Einschätzung der BNetzA, um eine bestimmungsgemäße WLAN-Nutzung handelt, ist, unserer Meinung nach, unzutreffend.

Zu einer Störung von bestimmungsgemäßer WLAN-Nutzung kann es aber zumindest dann kommen, wenn durch das Aussenden von Deauth-Paketen nicht nur der Verbindungsaufbau zu Rogue-Access-Points unterdrückt wird, sondern auch Netzwerkzugänge, die ohne Schädigungsabsicht errichtet wurden, „blockiert" werden.

Die Einstufung, dass Deauth-Pakete pauschal gegen die Allgemeinverfügungen verstoßen, lässt ungeachtet, dass WLAN-Deauther auch gegen gerade nicht bestimmungsgemäße WLAN-Nutzung, wie Rogue-Access-Points, eingesetzt werden können. Die Einschätzung der BNetzA in ihren bisherigen Stellungnahmen und Abmahnung ist somit undifferenziert. Nur der Einsatz von Deauth-Paketen gegen tatsächlich bestimmungsgemäße WLAN-Nutzung kann als relevante Störung gesehen werden. Dies kann zwar schon dann der Fall sein, wenn in einem „Deauth-Rundumschlag" alle umliegenden Netzwerkzugänge geblockt werden. Eine pauschale Annahme, dass WLAN-Deauther gegen die Allgemeinverfügung verstoßen, ist, unserer Einschätzung nach, jedoch falsch.
Dieser Umstand eröffnet zwei Lösungswege: Es kann schon gegen die recht unbestimmte Allgemeinverfügung vorgegangen werden oder es kann auf, nach unserer Ansicht, fälschlicherweise erlassene Konsequenzen der BNetzA eingegangen werden.

Die nicht näher definierte Verwendung des Begriffes „bestimmungsgemäße WLAN-Nutzung" könnte gegen das dem Art. 20 Abs. 3 Grundgesetz (GG) entspringende Bestimmtheitsgebot verstoßen. Zur Beseitigung der Allgemeinverfügungen in ihrer jetzigen Form kommt ein Widerspruch bzw. eine Anfechtung bzw. Neuregelung im Klageweg in Betracht. Allerdings ist die Rechts-

mittelfrist für die genannten Zuteilungen bereits erloschen. Der potentiell rechtswidrige Zustand ist somit hinzunehmen. Die BNetzA kann die Verfügungen allerdings noch einseitig zurücknehmen (für den Fall, dass es sich tatsächlich um rechtswidrige Verfügungen handelt, wäre § 48 VwVfG hierfür die Rechtsgrundlage). Für ein solches Vorgehen der BNetzA bestehen jedoch bisher keine Anhaltspunkte. Auch auf eine Beseitigung der problematisierten Passagen im Wege einer Neufassung der Verfügungen oder das Wiederaufgreifen des Verfahrens (§ 51 VwVfG) ist aktuell nicht zu hoffen. Die Erteilung von Abmahnungen und die Beantwortung von Anfragen, mit der Aussage, WLAN-Deauther verstoßen pauschal gegen die Allgemeinzuteilungen, senden diesbezüglich ein klares Signal der BNetzA.
Zur vollständigen Betrachtung der Problematik ist ferner die Auseinandersetzung mit den Konsequenzen eines Verstoßes gegen die Allgemeinzuteilungen unabdingbar.

IV. Konsequenzen bei Missachtung

Grundsätzlich führen Verstöße gegen Allgemeinverfügungen (also Verwaltungsakte) zur Durchsetzung dieser im Wege des Verwaltungszwanges nach § 6 Verwaltungs-Vollstreckungsgesetz (VwVG). Vorliegend wäre wohl das Zwangsgeld (§ 9 Abs. 1 lit. b VwVG) Mittel der Wahl. Ein Vollzug gegen juristische Personen des öffentlichen Rechts ist nach § 17 VwVG allerdings unzulässig. Bei Hochschulen handelt es sich regelmäßig um Körperschaften des öffentlichen Rechts. Ein Vollzug der Allgemeinverfügungen im Wege des Verwaltungszwangs scheidet somit aus. Möglich bleibt aber weiterhin die Einsetzung einer Fach- oder Rechtsaufsicht an den Hochschulen zur effektiven Einhaltung der Vorgaben der Allgemeinverfügungen.

Den Vorschriften des Telekommunikationsgesetzes (TKG) ist eine weitere mögliche Konsequenz zu entnehmen. Wenn das Verbot, die bestimmungsgemäße WLAN-Nutzung zu stören, als Nebenbestimmung im Sinne des § 60 Abs. 2 S. 1 TKG einzuordnen ist, kann ein Verstoß gegen diese Nebenbestimmung nach § 149 Abs. 2 Nr. 4 TKG ein Bußgeld von bis zu 100.000 € mit sich bringen. Ein drohendes Bußgeld nach den Vorschriften des TKG ist somit als reelle Konsequenz der Einstufung des genannten Verbots als Nebenbestimmung zu berücksichtigen.
Allerdings ist Folgendes zu bedenken: Werden Deauth-Pakete zielgerichtet und ausschließlich gegen Rogue-Access-Points und somit gegen Netzwerkzugänge mit Schädigungsabsicht eingesetzt, liegt, nach unserer Einschätzung, schon keine Störung bestimmungsgemäßer WLAN-Nutzung vor. Ein gerügter Verstoß gegen die Allgemeinverfügung der BNetzA wäre also verfehlt. Einem erteilten Bußgeldbescheid würde es danach an der Rechtsgrundlage fehlen und er wäre entsprechend durch Widerspruch und Klage anfechtbar.

V. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Auch wenn die Problematik der Rogue-Access-Points sich keineswegs auf Einrichtungen von Hochschulen beschränkt, ist die Bedrohung besonders für Hochschulen und Forschungseinrichtungen von erheblicher Relevanz. Der universitäre Alltag ist ohne flächendeckende Netzwerkzugänge undenkbar. Die meisten Studenten und Mitarbeiter loggen sich schon automatisch in das WLAN der Uni ein. Bei unzureichender Konfiguration der Endgeräte ist es für die Betreiber von Rogue-Access-Points ein Leichtes, die Daten der Nutzer auszulesen. Um sich solcher Angriffe zu erwehren, gibt es für Hochschulen zurzeit kaum einen effizienteren Weg als die Aussendung von Deauth-Paketen. Die pauschale Ablehnung von Deauth-Paketen durch die BNetzA und die drohenden Bußgelder machen dieser effizienten Vorgehensweise allerdings vorerst einen Strich durch die Rechnung. Ein Angreifen der Allgemeinzuteilungen der BNetzA verspricht keinen Erfolg. Allerdings sind aus ihnen folgende Konsequenzen bei zielgerichtetem Einsatz der WLAN-Deauthern gegen Access-Points mit Schädigungsabsicht nicht ohne Weiteres hinzunehmen.

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