infobrief recht DFN

1/2021
Januar 2021

Kein Anschluss unter dieser Nummer

BGH zur Störerhaftung eines Domain-Registrars für Urheberrechtsverletzungen

Manche mögen's transparent

Das Oberverwaltungsgericht Hamburg entscheidet, dass die Universität Hamburg die Quellen ihrer privaten Zuwendungen nicht nennen muss

Der Stand zwischen den Stühlen

Das Problem der praktischen Einordnung des Stands der Technik in der Datenschutzgrundverordnung

Kein Anschluss unter dieser Nummer

BGH zur Störerhaftung eines Domain-Registrars für Urheberrechtsverletzungen

von Marten Tiessen

Der einzig effektive Weg, gegen Urheberrechtsverletzungen im Internet vorzugehen, verläuft für Rechteinhaber manchmal nicht über den Websitebetreiber oder Host-Provider, sondern den Domainregistrar. Sie haben die Möglichkeit, die Verknüpfung der Website zur Domain zu unterbrechen und dadurch den Zugang Dritter zu illegalen Inhalten zu unterbinden. Der Bundesgerichtshof (BGH) hat in einem neuen Urteil Bedingungen aufgestellt, die für eine Haftung des Registrars vorliegen müsen. Diese Hürden sind so hoch, dass eine Anwendung für wissenschaftliche Urheber nur im Ausnahmefall in Betracht kommen dürfte.

I. Hintergrund

Für den reibungslosen Informationsaustausch im Internet sind verschiedene Akteure verantwortlich. Sofern man von Websites spricht, sind die Betreiber und häufig auch Nutzer der Website zwar diejenigen, die Inhalte ins Internet stellen (Content-Provider). Bevor die Inhalte aber überhaupt wahrgenommen werden können, sind zusätzliche Dienstleistungen anderer Anbieter erforderlich: Um die Inhalte einer Website speichern zu können, bedarf es Speicherkapazitäten, die auf den Webservern von Host-Providern bereitgestellt werden. Der Zugang zum Internet und die daran anschließende Datenübertragung werden wiederum von Access-Providern gewährleistet. Für einen flüssigen Informationsaustausch genügt allerdings nicht allein die Bereitstellung und Abrufbarkeit von Inhalten. Damit Websites zielgerichtet angesteuert werden können, bedarf es einer vereinfachten Auffindbarkeit der Inhalte. Diesem Umstand trägt das Domain-Name-System Rechnung, das eine Auflösung von Domainnamen zu IP-Adressen – ähnlich einer Telefonauskunft – ermöglicht. Domain-Namen müssen bei einer Registrierungsstelle (Registry), wie z.B. DENIC, eingetragen werden. Die Vermittlung zwischen dem Domainregister und dem Websitebetreiber übernehmen Registrare, wie z.B. GoDaddy. Gegen Gebühr beantragen sie die Eintragung einer Domain bei der Registry. Umgekehrt haben Registrare als Schnittstelle zwischen dem Domainregister und den Domaininhabern allerdings auch die Möglichkeit, die Auflösung der Verknüpfung zwischen Domain und Website zu veranlassen (Dekonnektierung). Diese kann notwendig sein, wenn die registrierte Domain hauptsächlich zu illegalen Zwecken genutzt wird.[1]

In der Vergangenheit hatten sich schon mehrere Gerichte mit der Haftung von Registraren bei Urheberrechtsverletzungen auf von ihnen vermittelten Websites beschäftigt.[2] Nun ist das erste höchstrichterliche Urteil zu dem Problem erschienen (Urteil vom 15.10.2020 – I ZR 13/19).

II. Störerhaftung der Registrare nach dem BGH

In dem Verfahren klagt eine Tonträgerherstellerin, die Inhaberin der ausschließlichen Verwertungsrechte eines Musikalbums ist, gegen die Beklagte, die als Registrar Domains für die Top-Level-Domain „com“ vermittelt. Zu den von der Beklagten vermittelten Websites gehört auch eine BitTorrent-Seite, über die das besagte Musikalbum unerlaubt heruntergeladen werden konnte. Damit die Rechtsverletzung unterbunden wird, verlangte die Klägerin von der Beklagten die Dekonnektierung der Website. Die Beklagte sah sich dagegen zu einem solchen Schritt nicht verpflichtet. Nachdem die Klägerin in den

1 Siehe zur Haftung des Domaininhabers und insbesondere des Admin-C Wellmann, Admin-C – Sag beim Abschied leise Servus, DFN-Infobrief 04/2020.

2 Siehe hierzu bereits ausführlich Tiessen, Wenn zwei sich freuen, haftet der Dritte, DFN-Infobrief 05/2019.

Vorinstanzen vor dem Landgericht und Oberlandesgericht Saarbrücken (Urteil vom 30.8.2017 - 7 O 17/15 und Urteil vom 19.12.2018 – 1 U 128/17) erfolgreich war, versuchte die Beklagte nun erfolgreich durch Revision ein abweichendes Urteil des BGH zu erreichen.

In seinem Urteil fasst der Gerichtshof zusammen, wer nach ständiger Rechtsprechung bei einer Rechtsverletzung im Internet als Störer in Anspruch genommen werden kann und welche unterschiedlichen Maßstäbe je nach Funktion und Tätigkeit für eine Haftung bestehen. Eine Haftung der Registry kommt beispielsweise nur in Sonderkonstellationen in Betracht, da ihre technische Arbeit für die Funktionsfähigkeit des Internets unabdingbar sind und nicht durch übermäßige Prüfpflichten erschwert werden soll. Für Host- oder Access-Provider liegen die Hürden einer Störerhaftung jedoch deutlich niedriger. Bei einem Hinweis auf eine Rechtsverletzung treffen sie Prüf- und Überwachungspflichten. Der Registrar haftet nach dem BGH wie ein Access-Provider. Bei der Bestimmung seiner Prüf- und Überwachungspflicht ist darauf zu achten, dass der Registrar durch seine administrativen Aufgaben ebenso eine für die Funktionsfähigkeit des Internets zentrale Rolle einnimmt. Es liegt also auch hier im Allgemeininteresse, wenn die Tätigkeit der Registrare nicht durch zu starke Prüf- und Überwachungspflichten gehemmt wird. Von den Inhalten der vermittelten Websites muss der Registrar daher grundsätzlich keine Kenntnis haben. Nur wenn er auf eine klare und ohne weiteres feststellbare Rechtsverletzung hingewiesen wird, muss er tätig werden. Eine gegenüber der Registry stärkere Prüfpflicht begründet der BGH mit der Gewinnerzielungsabsicht des Registrars, angesichts derer ein Vergleich mit dem Access-Provider zutreffender erscheint.

Der dadurch noch verbleibende nicht unerhebliche Prüf- und Überwachungsaufwand wird weiter dadurch eingegrenzt, dass der Registrar nur subsidiär haftet. Das bedeutet, dass gegen ihn als Störer nur vorgegangen werden kann, wenn die Rechtsverfolgung gegenüber dem Verletzer selbst oder demjenigen, der ihn durch Dienstleistungen unterstützt hat, wie z. B. der Host-Provider, bereits gescheitert ist. Diese Subsidiarität ist nach dem BGH wesentliches Element der Registrarhaftung und verdeutlicht, dass diese nur ein letztes Mittel der Rechtsdurchsetzung sein soll. Die vorherige Instanz hatte im Gegensatz zum BGH noch keine subsidiäre Haftung des Registrars angenommen, weil er aufgrund seiner Vertragsbeziehungen mit dem Domaininhaber in einem Lager stünde und somit unmittelbar in Anspruch genommen werden könne.

Damit es nicht zu einem Overblocking kommt, fordert der BGH außerdem, dass die Inhalte der Website weit überwiegend illegal sein müssen, bevor die Dekonnektierung der Website verlangt werden kann. Sowohl die erfolglose Inanspruchnahme vorrangiger Haftungsgegner als auch die Zusammensetzung der Website aus illegalen Inhalten müssen sich bereits aus dem Hinweis des Rechteinhabers ergeben. Nur wenn der Rechteinhaber diese Informationsobliegenheit erfüllt hat, kann er die Dekonnektierung beanspruchen. Der BGH konnte in diesem Fall gerade nicht abschließend feststellen, ob die Klägerin vorher erfolglos gegen den Betreiber der Internetseite und Host-Provider vorgegangen ist, und die Beklagte darauf hingewiesen hat. Daher verwies der Gerichtshof das Verfahren zurück an die vorherige Instanz zur endgültigen Entscheidung.

III. Praxishinweise

Der BGH hat in seinem Urteil klare Voraussetzungen für eine Haftung des Registrars benannt, deren Nachweis der Verletzte erbringen muss. Diese Voraussetzungen stellen erhebliche Hürden für die Rechtsverfolgung von Urheberrechtsverstößen dar, sind aber erforderlich, um der im Allgemeininteresse liegenden Funktion des Registrars gerecht zu werden. Durch extensive inhaltliche Prüfpflichten würde die Arbeit des Registrars unnötig erschwert werden. Hingegen ist es dem Rechteinhaber zuzumuten, zunächst gegen den unmittelbaren Verletzer und seinen Host-Provider vorzugehen. Wollen Urheber an Hochschulen und Forschungseinrichtungen eine Rechtsverletzung im Internet abstellen, kann der Registrar durch die Dekonnektierung der Website zwar effektiv Abhilfe schaffen, eingefordert werden kann sie aber nur in absoluten Ausnahmefällen. Sofern es um wissenschaftliche Publikationen geht, liegen die Rechte in der Regel auch nicht beim Wissenschaftler, sondern beim Verlag, so dass auch nur letzterer gegen eine Urheberrechtsverletzung vorgehen kann. Denkbar wäre insbesondere ein Vorgehen gegen sogenannte Schattenbibliotheken, die unerlaubt urheberrechtlich geschütztes Material ins Netz stellen. Das Bestreben großer Verlage, gegen die Websitebetreiber oder die Host-Provider von solchen Schattenbibliotheken vorzugehen, hat sich in der Vergangenheit als wenig erfolgsversprechend herausgestellt. Die Möglichkeit, den Registrar in Anspruch zu nehmen, erscheint dagegen zunächst vielversprechend. Allerdings bleibt auch hier das grundsätzliche Problem, dass sowohl Host-Provider als auch Registrare austauschbar sind. So kann die Website zu

einer neuen Domain migrieren, die durch einen anderen Registrar vermittelt wird. Die Durchsetzung etwaiger Ansprüche wird zudem erschwert, wenn sich die Registrare im Ausland befinden. Ob der Schaden den Aufwand der Rechtsverfolgung rechtfertigt, mag jeweils im Ermessen des Rechteinhabers liegen.

Manche mögen's transparent

Das Oberverwaltungsgericht Hamburg entscheidet, dass die Universität Hamburg die Quellen ihrer privaten Zuwendungen nicht nennen muss

von Nicolas John

Nachdem die Universität Hamburg vom Verwaltungsgericht (VG) Hamburg (Urt. v. 21.3.2018; Az.: 17 K 1459/16) verurteilt wurde, Informationen über die Identitäten von Zuwendungsgebern dem Kläger zur Verfügung zu stellen, hat nun das Oberverwaltungsgericht (OVG) Hamburg (Urt. v. 25.11.2020; Az.: 3 Bf 193/18) das Urteil auf die Berufung der Universität Hamburg hin abgewiesen. Streitgegenständlich waren dabei die Bestimmungen des Hamburgischen Transparenzgesetzes (HmbTG), die das OVG im vorliegenden Fall für einschlägig hielt und mit deren Befassung sich der nachfolgende Beitrag beschäftigt.

I. Hintergrund

Die Transparenz- und Informationsfreiheitsgesetze der Länder dienen dem Zugang der Bürger zu staatlichen Informationen. Der normierte Anspruch auf amtliche Informationen soll dabei Kontrollen ermöglichen, Korruption verhindern und dadurch das Vertrauen der Bürger in den Staat verbessern und stärken. Auf Bundesebene gilt für den Informationszugang zu amtlichen Informationen gegenüber Bundesbehörden und sonstigen Bundesorganen das Informationsfreiheitsgesetz (IFG). Für Landesbehörden sind hingegen die jeweiligen Länderregelungen maßgeblich, wobei es hier erhebliche Unterschiede in deren Ausgestaltung gibt. So haben Bayern, Niedersachsen und Sachsen bislang keine gesetzlichen Regelungen hinsichtlich eines Informationszugangs erlassen, während die überwiegende Zahl der Länder wie beispielweise Nordrhein-Westfalen, Hessen oder Baden-Württemberg Informationsfreiheitsgesetze erlassen haben, welche die Herausgabe von Informationen auf Antrag regeln. Daneben gelten in einigen Ländern (Bremen, Hamburg, Rheinland-Pfalz und Thüringen) Transparenzgrundsätze, welche die Behörden zusätzlich zur eigenständigen Veröffentlichung von zentralen Daten verpflichten, wie beispielweise Verträge der Daseinsvorsorge, in Auftrag gegebene Gutachten oder Subventions- oder Zuwendungsvergaben.

II. Sachverhalt und Gang des Verfahrens

Der Beginn des Verfahrens liegt bereits im Jahr 2015. Damals verlangte der Kläger von der Universität Hamburg auf Grundlage des Hamburgischen Transparenzgesetzes die Zusendung einer Übersicht aller in den Jahren 2012, 2013 und 2014 erhaltenen, den Wert von 1.000 EUR übersteigenden Sponsoring Leistungen, Spenden, Schenkungen und Werbezuwendungen unter Nennung der Namen der jeweiligen Geldgeber, der Höhe der finanziellen Zuwendung sowie der Art und des Werts der materiellen Zuwendung. Die Universität Hamburg kam diesem Begehren nur teilweise nach und übersandte die erbetenen Informationen zu einem großen Teil ohne Nennung der Namen der Zuwendungsgeber, wenn diese eine Zustimmung zur Veröffentlichung ihrer Namen nicht erteilt hatten.

Die Universität Hamburg begründete die Nicht-Nennung der Zuwendungsgeber unter Verweis auf die Möglichkeit der Spender, den Vertragsschluss von der Verweigerung der Namensveröffentlichung abhängig zu machen. Der hierauf begründete Vertrauenstatbestand gebiete es, die vertragliche Vereinbarung als maßgeblich zu betrachten. Auch überwogen die Interessen des Vertragspartners aus Sicht der Beklagten ihn diesem Fall. Im Übrigen sei die Universität Hamburg nicht zur Auskunft verpflichtet, da die Ausnahmeregelung des § 5 Nr. 7 HmbTG, welche die Informationspflicht bei Grundlagenforschung oder

anwendungsbezogene Forschung ausschließt, an dieser Stelle gelte. Außerdem müsste bei einer Verpflichtung zur Veröffentlichung der Namen gegen den Willen der Zuwendungsgeber mit einem Absehen von weiteren Zuwendungen zu rechnen sein.

Der Kläger wendete dagegen ein, dass der Ausnahmetatbestand nicht einschlägig sei, da durch die Informationsherausgabe die Forschungsfreiheit nicht berührt werde und verlangte daraufhin weiterhin die Informationsherausgabe.

III. Entscheidung des VG Hamburg

Nach erfolglosem Widerspruch klagte der Kläger vor dem VG Hamburg auf die Verpflichtung der Universität Hamburg, die begehrten Informationen zur Verfügung zu stellen. Diesem Klagebegehren kam das VG Hamburg nach und verurteilte die Universität Hamburg zur Herausgabe der Informationen mit Urteil vom 21. März 2018 (Az.: 17 K 1459/16). Das VG Hamburg sah den Ausnahmetatbestand des § 5 Nr. 7 HmbTG als nicht erfüllt an, da dieser nur den Kernbereich der Forschungsfreiheit schütze. Die Gewährung von Informationen über erfolgte Zuwendungen berühre dabei nicht die „wissenschaftsrelevanten" Angelegenheiten der Beklagten, da sie hierdurch nicht in ihrer Freiheit, über das Ob und Wie der Durchführung und der Gewinnung von Forschungsergebnissen zu entscheiden, beeinträchtigt würde. Dass tatsächlich Spender zukünftig nicht mehr bereit seien, die Beklagte finanziell zu unterstützen, habe die Universität Hamburg nicht ausreichend konkret darlegen können.

Zudem könne nach der Ansicht des VGs die Universität Hamburg durch die vertragliche Vereinbarung mit dem Zuwendungsgeber, die Identität nicht zu nennen, keinen Vertrauenstatbestand schaffen, welcher nicht mit den gesetzlichen Tatbeständen vereinbar sei. Den vertraglichen Ausschluss der Auskunftspflicht sehe das HmbTG gerade nicht vor.

IV. Entscheidung des OVG Hamburg

Gegen die Entscheidung des VG Hamburg legte die Universität Hamburg Berufung vor dem OVG Hamburg ein. Sie war weiterhin der Auffassung, dass der Ausnahmetatbestand des § 5 Nr. 7 HmbTG entgegen des Urteils des VG Hamburgs weit zu verstehen sei und nicht nur den Kernbereich der Forschungsfreiheit umfasse.

Dieser Argumentation schloss sich das OVG Hamburg an und änderte das erstinstanzliche Gericht des VG Hamburgs mit Urteil vom 25. November 2020 (Az.: 3 Bf 193/18) dahingehend ab und wies die Klage des erstinstanzlichen Klägers ab.

Die Ausnahmevorschrift des § 5 Nr. 7 HmbTG sei nicht nur auf den Kernbereich der Wissenschaftsfreiheit beschränkt. Sie erfasse auch unmittelbar wissenschaftsrelevante Angelegenheiten und insoweit auch Informationen über Drittmittel zu Forschungszwecken. Hierunter fallen vorbereitende und unterstützende Tätigkeiten, wie die organisatorische Betreuung und Sicherung der Durchführung von Forschungsvorhaben, einschließlich der haushaltsmäßigen Betreuung. Über die Angabe eines Verwendungszwecks stelle die Spende eine grundlegende Weiche für die Durchführung von Forschungsprojekten und damit für die Gewinnung von Forschungsergebnissen dar. Mit Annahme einer Zuwendung werde sie damit im Bereich der Forschung tätig. Der erstinstanzliche Kläger habe daher keinen Anspruch auf Informationen über die von der Universität Hamburg erhaltenen finanziellen Zuwendung, insbesondere auch nicht auf die Nennung der Namen.

V. Fazit und Konsequenzen für Hochschulen

Drittelmittelprojekte an Hochschulen und Forschungseinrichtungen sind bundesweit gängige Praxis. Hierdurch lassen sich oftmals die Interessen des Zuwendungsgebers, aber auch die der Hochschule sinnvoll verbinden und stellen daher ein wirkungsvolles Werkzeug dar, um einzelne Forschungsgebiete zu bereichern. Inwieweit die jeweilige Hochschule oder Forschungseinrichtung allerdings Veröffentlichungs- oder Informationspflichten unterliegt, ist Sache der jeweiligen Landesvorschriften.

Daher muss darauf hingewiesen werden, dass im Urteil des OVG Hamburg nur das Hamburgische Transparenzgesetz Anwendung finden konnte und daher das Urteil für andere Bundesländer kein unmittelbares Präjudiz bildet. Dennoch finden sich vergleichbare Ausnahmeregelungen in den Transparenz- bzw. Informationsfreiheitsgesetzen der anderen Bundesländer. Beispielsweise gilt das Informationsfreiheitsgesetz

von Nordrhein-Westfalen (IFG-NRW) gemäß § 2 Abs. 3 IFG-NRW nicht „im Bereich von Forschung, Lehre, Leistungsbeurteilung und Prüfung“. Genauso ist der Anwendungsbereich des Landesinformationsfreiheitsgesetzes Baden-Württemberg (LIFG-BW) gemäß § 2 Abs. 3 Nr. 1 LIFG-BW nicht eröffnet, „soweit Forschung, Kunst, Lehre, Leistungsbeurteilungen und Prüfungen betroffen sind“.

Soweit Landesgesetze also ähnliche Ausnahmeregelungen hinsichtlich der Forschung beinhalten, ist zumindest denkbar, dass auch hier die (Ober-) Verwaltungsgerichte den Begriff der Forschung nicht nur auf den Kernbereich beschränken und die Erwägungen des OVG Hamburgs teilen werden. Die Informationspflicht würde sich dann auch hier nicht auf die Identität der Zuwendungsgeber erstecken, soweit dies von ihnen nicht erwünscht ist. Doch ist stets der Einzelfall zu betrachten und insbesondere die geltenden Landesnormen zu studieren und anzuwenden.

So ist es beispielsweise in Bremen gänzlich anders geregelt: Hier verlangt § 1 Abs. 1a Bremer Informationsfreiheitsgesetz (BremIFG) i.V.m. § 75 Abs. 6 Bremisches Hochschulgesetz (BremHG) von Hochschulen die Führung einer öffentlich zugänglichen Forschungsdatenbank für Drittmittelprojekte, welche auch die Identität der Drittmittelgeber umfasst.

Wieder andere Informationsfreiheitsgesetze sehen keine Einschränkungen hinsichtlich der wissenschaftsrelevanten Angelegenheiten der Hochschulen vor. Inwieweit man sich hier auf andere Normen zum Schutz der Identität von Spendern berufen kann, ist dann erst Recht Frage des Einzelfalls und der jeweiligen Landesvorschriften.

Der Stand zwischen den Stühlen

Das Problem der praktischen Einordnung des Stands der Technik in der Datenschutzgrundverordnung

von Owen Mc Grath

Die Einhaltung der Vorgaben einer rechtmäßigen Verarbeitung im Sinne der DSGVO bereitet sowohl Praktikern als auch Theoretikern immer wieder Kopfzerbrechen. Sei es die Suche nach dem einschlägigen Erlaubnistatbestand oder die Einordnung der Grundsätze des Art. 5 DSGVO. Absolute Klarheit über den rechtlichen Rahmen der konkreten Verarbeitung personenbezogener Daten fehlt regelmäßig.
Doch nicht nur die rechtlichen Rahmenbedingungen sorgen für Fragen, auch der nicht weiter definierte Begriff des Stands der Technik in Art. 32 Abs. 1 und 25 Abs. 1 DSGVO bereitet Schwierigkeiten bei der Beachtung und Umsetzung und soll daher im folgenden Beitrag erörtert werden.

I. Gesetzliche Anknüpfung

Art. 25 DSGVO verlangt von dem Verantwortlichen die Berücksichtigung des Standes der Technik bei der Implementierung geeigneter, den Grundsätzen einer rechtmäßigen Datenverarbeitung entsprechender Maßnahmen. Art. 32 DSGVO verlangt ebenfalls die Berücksichtigung des Stands der Technik bei der Festlegung angemessener Sicherheitsmaßnahmen, welche die Verarbeitungen personenbezogener Daten schützen. Die notwendigen Maßnahmen erfahren bereits in den Erwägungsgründen zur DSGVO eine weitere Konkretisierung.[1] Der Stand der Technik wird allerdings auch hier nicht näher beleuchtet.

Auch außerhalb der DSGVO wird der Begriff Stand der Technik im Gesetzestext verwendet. Neben der Anführung im Bundesdatenschutzgesetz (BDSG) wird auch in datenschutzfremden Rechtsbereichen der Stand der Technik als abstrakte Anforderung gesetzt. So zum Beispiel im Bundesimmissionsschutzgesetz (BImSchG) und Telemediengesetz (TMG).

II. Warum wird der Gesetzgeber nicht konkreter?

Der Gesetzgeber bedient sich grundsätzlich allgemeiner Begriffe. Durch eine abstrakte Regelung wird sichergestellt, dass eine Vielzahl von konkreten Fällen in den Anwendungsbereich des Gesetzes fallen. So sind Gesetze als abstrakt-generelle Regelungen einzuordnen. Maßnahmen der Verwaltung hingegen sind zumeist konkret-individuelle, also auf den Einzelfall zugeschnittene Regelungen. In manchen Bereichen des Gesetzes werden Begriffe durch sog. Legaldefinitionen näher konkretisiert. Im Weiteren ist es Aufgabe der Rechtsprechung, Rechtspflege, Lehre und Forschung, Definitionen und Konkretisierungen der abstrakten Begriffe (sog. unbestimmte Rechtsbegriffe) zu entwickeln.

Gerade im Technikumfeld und insbesondere im Bereich der Datenverarbeitungen steht die Legislative vor einem großen Problem. Die Entwicklungen der Technik sind so rasant, dass nähere Definitionen, die Anwendbarkeit des einschlägigen Gesetzes obsolet machen würden. Die Beschreibung des bestehenden Standes der Technik in einer aktuellen Gesetzesfassung beispielsweise wird sich zügig als überholt herausstellen und eine Anpassung des Gesetzes erfordern. Nur so könnte die neue technische Situation sachgerecht geregelt werden. Eine solche Anpassung müsste einen regelmäßig langwierigen

1 Erwägungsgründe 78, 83.

parlamentarischen Prozess durchlaufen. Bis zur Geltung des neuen Gesetzes wird sich der Stand der Technik auf ein Neues verschoben haben. Der gleiche Prozess würde von Neuem beginnen.

Die Verabschiedung zu konkreter Normen würde mit den Entwicklungen der technischen Welt zunehmend schlechter Schritt halten können. Folge sind Gesetze mit weiten Formulierung, die näherer Definition und Interpretation bedürfen.

III. Was meint der Stand der Technik?

Nachdem Klarheit über die Notwendigkeit von abstrakten Formulierungen in Gesetzen besteht, stellt sich nun die konkrete Frage nach der Bedeutung des Standes der Technik in der Systematik der DSGVO. Wortwörtlich liegt das Verständnis als „aktuellster Stand der Technik“ nahe. Demzufolge wären Erwägungen der Datensicherheit immer im Lichte des aktuell technisch Machbaren zu treffen. Im Ergebnis wären Verantwortliche von Datenverarbeitungsprozessen so allzu schnell verpflichtet, Unsummen in technische Neuerungen zu investieren, welche sich gegebenenfalls aufgrund ihrer fehlenden Bewährung als dennoch unbrauchbar herausstellen.

Richtigerweise fordern Art. 32 und 25 DSGVO aber nicht stets die neueste Technik bei der Umsetzung geeigneter technischer und organisatorischer Maßnahmen. Vielmehr soll gerade auch die Bewährtheit der Maßnahmen Berücksichtigung finden. Damit sind nur solche technischen Errungenschaften für den Stand der Technik maßgebend, die nach gesicherten Erkenntnissen wirksam sind. Die Mischung aus Bewährtem und technisch Umsetzbarem formt erst den Stand der Technik im Sinne der DSGVO.

Selbst nach dieser Eingrenzung befinden wir uns noch im abstrakten Bereich. Eine tatsächliche Konkretisierung der durchzuführenden Maßnahmen nach Stand der Technik lässt sich allerdings auch nur im Einzelfall durchführen und würde selbst in Beispielen den Rahmen dieser Ausführungen sprengen.

Orientierungshilfe zur Einordnung der zu treffenden Maßnahmen können Veröffentlichungen in den jeweilig relevanten Fachbereichen und der Austausch mit anderen Verantwortlichen geben. Aber auch von offizieller Seite wird der Phrase „Stand der Technik“ Leben eingehaucht. Die Europäische Agentur für Netz- und Informationssicherheit beispielweise gibt schon auf europäischer Ebene mit ihren Veröffentlichung Werkzeuge an die Hand, die die Konkretisierung des Stands der Technik im Einzelfall ermöglicht.[2] Auch das Bundesamt für Sicherheit in der Informationstechnik,[3] die Datenschutzbehörden der Länder sowie Fachverbände stellen mit ihren Veröffentlichungen die Weichen zur genaueren Einordnung.

Nicht aus dem Blick zu verlieren ist bei jeder Maßnahme im Sinne der Art. 25 und 32 DSGVO, dass der Stand der Technik kein starrer Begriff ist, sondern sich stets fortentwickelt. Was vor wenigen Monaten noch Stand der Technik war, kann schnell abgelöst werden. „Veraltete“ Maßnahmen stellen sich damit als unzureichend im Lichte der DSGVO dar. Derartig gesicherte bzw. eben ungesicherte Datenverarbeitung bergen das Risiko einer unrechtmäßigen Verarbeitung und entsprechender Konsequenzen in Form von Abmahnungen und Bußgeldern.

IV.Fazit und Bedeutung für wissenschaftliche Einrichtungen

Wie regelmäßig im Datenschutzrecht sind auch Hochschulen und wissenschaftliche Einrichtungen von den gesetzlichen Vorgaben betroffen. Alle Verantwortlichen haben bei Verarbeitungen personenbezogener Daten die nach Art. 25 und 32 DSGVO relevanten Maßnahmen zu treffen. Der Stand der Technik ist als Auswahlkriterium der Maßnahmen unbedingt zu beachten. Erforderliche technische und organisatorische Maßnahmen sollten nicht schlicht nach eigenem Ermessen ausgewählt werden, sondern nur unter Berücksichtigung der genannten Quellen, umso den gesetzlichen Vorgaben Genüge zu tun. Weitergehend ist die Aktualität der Maßnahmen nicht aus dem Blick zu verlieren. Die Vereinbarkeit von gewählten Maßnahmen mit dem aktuellen Stand der Technik sollte regelmäßig überprüft werden.

2 Die Veröffentlichungen der ENISA sind abrufbar unter: https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

3 Die technischen Richtlinien des BSI sind abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

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