DFN
infobrief recht

3 / 2021
März 2021

Error 403. Zugriff verweigert.
Der BGH entschied, dass sich ein Systemadministrator strafbar macht, wenn er seine Zugriffsbefugnisse missbraucht

Das Dilemma der Digitalen Dienste
Ein Überblick über die Umsetzung der Digitale-Inhalte-Richtlinie

Digital Services Act: Das Plattformgrundgesetz?
Die Europäische Union gegen die Meinungsmacht der Plattformen

Error 403. Zugriff verweigert.

Der BGH entschied, dass sich ein Systemadministrator strafbar macht, wenn er seine Zugriffsbefugnisse missbraucht

von Nicolas John

Auch unbefugte Zugriffe innerhalb des Netzwerks durch einen Systemadministrator können den Straftatbestand des § 202a Abs. 1 Strafgesetzbuch (StGB) erfüllen. Der Bundesgerichtshof (BGH) entschied in seinem Beschluss vom 13. Mai 2020 (Az.: 5 StR 614/19), dass ein Konto auch gegen den unberechtigten Zugang gesichert ist, wenn der Systemadministrator aufgrund seiner Stellung ungehindert auf dieses zugreifen kann.

I. Hintergrund

Gemäß § 202a StGB macht sich strafbar, wer sich oder einem anderen unter Überwindung der Zugangssicherung Zugang zu Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Solche Zugriffe erfolgen typischerweise durch nichtberechtigte Dritte, die eine besondere Zugangssicherung überwinden, um sich Zugriff zu den Daten zu verschaffen. Beim „Hacking" stellt sich beispielsweise die Situation regelmäßig so dar, dass ein Dritter unter Überwindung von Zugangssperren wie Passwörtern, Sicherheitsfragen oder Tan-Verfahren unbefugt auf fremde Daten zugreift. So verschaffen sich Cyberkriminelle oftmals Zugang zu fremden IT-Systemen, um die darin enthaltenen Daten einzusehen und weiterzugeben. Meist findet der Zugriff auf die Daten von einem Dritten statt, der außerhalb des Systems steht.

Untypischer ist die Situation, dass der Datenzugriff von einer Person aus dem Netzwerk ausgeht. Beispielsweise Mitarbeiter eines Unternehmens, Systemadministratoren oder andere Nutzer des Netzwerks, die zwar grundsätzlich auf bestimmte Datensätze im Netzwerk zugreifen dürfen, jedoch ihre Befugnisse mit einem Zugriff auf geschützte Daten überschreiten. Ob die Frage nach der Strafbarkeit in diesem Fall anders bewertet werden muss, beschäftigte den BGH in seinem Beschluss vom 13. Mai 2020 (Az.: 5 StR 614/19).

II. Sachverhalt

In diesem Beschluss musste sich der BGH mit der Revision eines Systemadministrators beschäftigen, welcher zuvor vom Landgericht (LG) Berlin (Urt. v. 10.04.2019, Az.: 222 Js 1953/12) unter anderem wegen des Ausspähens von Daten gem. § 202a StGB verurteilt worden war.

Dem Sachverhalt lag die Administratorenstellung des Angeklagten im Bundesministerium für Gesundheit zugrunde. Durch diese Stellung hatte der Angeklagte nach dem Einloggen mit seinem Passwort im zentralen Verzeichnis des Systems Zugriff auf alle E-Mailkonten und deren gespeicherte Inhalte. Das Konto, das er hierzu verwendete, wurde regelmäßig für Schulungszwecke verwendet und das Passwort war unter den Administratoren allgemein bekannt. Nachdem dieser Sicherheitsmangel bekannt wurde, änderte das Ministerium die Zugriffsrechte der Administratoren, damit der unbeschränkte Zugriff auf die E-Mail-Konten nicht mehr möglich war. Doch trotz dieser Änderungen war es dem Angeklagten möglich, mittels Systemeinstellungen weiterhin Zugriff auf die passwortgeschützten Postfächer der Ministeriumsmitarbeiter zu erlangen.

Diese Möglichkeit nutzte der Angeklagte dahingehend, dass er in den Jahren 2009 bis 2012 auf bestimmte öffentliche und auch private Postfächer zugriff, welche ihm von einem Dritten zuvor benannt worden waren, um anschließend die hierdurch erlangten Datensätze an diesen zu verkaufen. Bei den betrof-

fenen Nutzern handelte es sich vor allem um Minister, Staatssekretäre, Abteilungs- und Referatsleiter und die Leiterin des Leitungsstabes des Ministeriums.

III. Entscheidung des BGH

Der BGH bestätigte die Entscheidung des LG Berlins und bejahte die Strafbarkeit des Systemadministrators wegen Ausspähens von Daten i.S.d. § 202a Abs. 1 StGB.
Dass die Daten nicht für ihn bestimmt waren, ergibt sich für den BGH bereits aus der Passwortsperre der E-Mail-Konten. Die begrenzten Zugriffsrechte als Administrator umfassten gerade nicht das aufgabenunabhängige Lesen und Kopieren von E-Mails aus den persönlichen Konten der Mitarbeiter, sondern waren allein auf technische Aufgaben zur Verwaltung des Netzwerks beschränkt, wie beispielsweise die Wartung des Netzwerks.

Weiter legt der BGH ausführlich dar, dass die Daten gegen den unberechtigten Zugang i.S.d. § 202a StGB besonders gesichert waren. Grundsätzlich ist dies der Fall, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Durch die Sicherung muss der Berechtige sein spezielles Interesse an der Geheimhaltung dokumentieren. Vorliegend waren die Zugänge zu den E-Mail-Konten durch Passwörter gesichert, welche als Zugangssicherung i.S.d. § 202a Abs. 1 StGB ausreichen. Darüber hinaus ist nach Ansicht des BGH nicht darauf abzustellen, wie leicht Eingeweihte oder Experten auf die Daten zugreifen können, sondern allein auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter. Es sei auch nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt. Dass es dem Angeklagten mit nur wenigen Systemeinstellungen möglich war, in die Konten Einblick zu erlangen, sei daher unerheblich.

Im Übrigen entschied der BGH im Sinne des Gesetzgeberwillens, indem er das Merkmal der Überwindung der Zugangssicherung bejahte. Nach der Gesetzesbegründung muss die Überwindung der Zugangssicherung typischerweise, also nach Auffassung des Senats unabhängig von spezifischen Möglichkeiten des konkreten Täters, einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordern. Daraus folgert der BGH zwei Aspekte: Zum einen, dass durch das Erfordernis der Überwindung Bagatellfälle ausgeschieden werden sollen und dem Täter eine deutliche Schranke gesetzt werden soll, deren Überwindung seine strafwürdige kriminelle Energie manifestiert. Soweit der Täter gezwungen ist, eine Zugangsart zu wählen, welche der Berechtigte verhindern wollte, sei das Tatbestandsmerkmal nach dem Willen des Gesetzgebers erfüllt.

Zum anderen sei der Tatbestand nach den Ausführungen des BGH auch dann erfüllt, wenn die Zugangssicherung aufgrund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand überwunden wird. Für den betroffenen Nutzer sei es für sein Geheimhaltungsinteresse unerheblich, ob die Sicherung schnell oder langsam, mit viel oder wenig Aufwand überwunden wird. Nur Sachverhalte, in denen es jedermann ohne weiteres möglich sei, die Zugangssicherung zu überwinden, sollen anhand des Merkmals der Überwindung ausgeschlossen werden können. Im vorliegenden Fall habe der Angeklagte daher die Zugangssicherung i.S.d. § 202a StGB überwunden, obwohl ihm dies mit wenigen Klicks in den Systemeinstellungen möglich war. Der Passwortschutz sowie die vorgenommene Beschränkung der Administratorenrechte zeige erkennbar das formelle Geheimhaltungsinteresse der Verfügungsberechtigten.
Abschließend bejahte der BGH ebenfalls, dass der Zugriff unbefugt erfolgte, denn dem Angeklagten waren derartige Zugriffe auf die E-Mail-Konten ausdrücklich verboten und nicht von seinen Aufgaben als Systemadministrator umfasst.

IV. Fazit und Konsequenzen für Hochschulen

Der Beschluss des BGH zeigt anschaulich, dass die Strafbarkeit des § 202a StGB nicht nur für Cyberangriffe von außen gegen das Netzwerk eine Rolle spielt, sondern auch für Täter innerhalb der Netzwerkstrukturen zur Anwendung kommen kann. Der Schutz der Daten ist daher auch im internen Bereich nicht zu vernachlässigen. Der BGH hat klargestellt, dass schon der Passwortschutz als Zugangssicherung genügt, um den Tatbestand zu erfüllen. Daher sollte nicht auf solche Schutzmechanismen verzichtet werden. Darüber hinaus zeigt der Beschluss, dass klare Verfahren für die Systemadministration detailliert festgelegt werden sollten, damit hier nicht versehentlich unerkannte Sicherheitslücken entstehen können.

Zugriffsberechtigungen sollten zudem selbstverständlich nur für die vereinbarten zulässigen und erforderlichen (techni-

schen) Zwecke verwendet werden. Neben Fragen des Datenschutzes[1] ist auch im Strafrecht gerade im Bereich einer (erlaubten) Privatnutzung der E-Mail-Konten oder Computer hier genau darauf zu achten, wie weit Zugriffsrechte erteilt werden können oder gerechtfertigt sind. Wer verfügungsbefugt ist, hängt grundsätzlich davon ab, wer die Daten erstellt und speichert. Bei dienstlichen Dateien ist dies zwar der Arbeitnehmer, doch unterliegt dieser dem Weisungsrecht des Arbeitgebers, bzw. Treuepflichten des Dienstherrn. Bei Vorliegen privater Daten der Mitarbeiter können diese dem Schutz des § 202a StGB unterfallen, soweit alle Tatbestandsmerkmale vorliegen. Aus diesen Gründen ist anzuraten, dass beispielsweise erforderliche Wartungsarbeiten im Vorfeld mit den betroffenen Nutzern abgesprochen werden und die Zustimmung hierzu eingeholt wird, um einem Miss- oder Fehlgebrauch der Zugangsdaten so weit möglich zuvorzukommen.

1 Vgl. Tiessen, All work and no play…, DFN-Infobrief Recht 11/2019; John, Möge die Firewall mit dir sein, DFN-Infobrief Recht 4/2020.

Das Dilemma der Digitalen Dienste

Ein Überblick über die Umsetzung der Digitale-Inhalte-Richtlinie

von Owen Mc Grath

Digitale Inhalte und Dienste sind mittlerweile zentraler Teil unseres alltäglichen Nutzungs- und Konsumverhaltens. Dennoch finden sich bisher keine gesonderten Regelungen zu Verbraucherverträgen über digitale Dienstleistungen im nationalen Recht. Mit der Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (Digitale-Inhalte-Richtlinie) versucht der Gesetzgeber, diesen Missstand zu beheben. Derzeit liegt neben dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) auch der Gesetzesentwurf der Bundesregierung vor.

I. Grundlagen zur Richtlinie

Bisher gibt es im deutschen Zivilrecht keine Regelungen, die die Besonderheiten digitaler Produkte in Konstellationen zwischen Unternehmern und Verbrauchern (Verbraucherverträge)[1] berücksichtigen. Herkömmliche Regeln des Verbraucherschutzes finden bis dato Anwendung. Für den Verkauf digitaler Güter und die Vornahme digitaler Dienstleistungen gelten die gleichen gesetzlichen Rahmenbedingungen, wie für herkömmliche Waren oder Dienstleistungen.

Während andere Mitgliedsstaaten der EU auf diesen Umstand im eigenen Land reagierten und eigene Regelungen schufen, blieb der deutsche Gesetzgeber untätig. In der Absicht, einen Flickenteppich an europäischen Regelungen zu verhindern und eine Harmonisierung des Verbrauchervertragrechts in Bezug auf digitale Produkte in der EU zu erreichen,[2] erließ das Europäische Parlament am 20. Mai 2019 die Digitale-Inhalte-Richtlinie (RL (EU) 2019/770).

Bis Mitte dieses Jahres haben die Mitgliedsstaaten die Regelungen der Richtlinie in nationales Recht umzuwandeln, welches dann zu Beginn 2022 anzuwenden ist. Nachdem das BMJV im November bereits einen Referentenentwurf vorgelegt hat, erschien zu Beginn des Jahres nun auch der Gesetzesentwurf der Bundesregierung.

II. Was sind digitale Inhalte und Dienstleistungen?

Digitale Dienstleistungen und Inhalte trennscharf final zu definieren oder aufzuzählen, ist weder besonders zielführend noch Absicht des Gesetzgebers. Die Entwicklungen der digitalen Welt sind mittlerweile derartig rasant, dass eine abschließende Eingrenzung der zu regelnden Fälle schnell zu eng sein könnte. Derzeit sollen sich die Regelungen „unter anderem auf Computerprogramme, Anwendungen, Videodateien, Audiodateien, Musikdateien, digitale Spiele, elektronische Bücher und andere elektronische Publikationen und auch digitale Dienstleistungen erstrecken, die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form sowie den Zugriff auf sie ermöglichen, einschließlich Software-as-a-Service, wie die gemeinsame Nutzung von Video- oder Audioinhalten und andere Formen des Datei-Hosting, Textverarbeitung oder Spiele, die in einer Cloud-Computing-Umgebung und in sozialen Medien angeboten werden“.[3]

1 Der Begriff des Unternehmers und Verbrauchers ist in §§ 13, 14 BGB geregelt.

2 RefE DID-RL, S.1; RegE DID-RL, S.1.

3 ErwGr. 19 RL (EU) 2019/770

Im Regierungsentwurf werden in § 327 Abs. 2 Bürgerliches Gesetzbuch-Entwurf (BGB-E) digitale Inhalte und Dienstleistungen folgendermaßen definiert: „Digitale Inhalte sind Daten, die in digitaler Form erstellt und bereitgestellt werden. Digitale Dienstleistungen sind Dienstleistungen, die dem Verbraucher

1. die Erstellung, die Verarbeitung oder die Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen, oder
2. die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen." Ferner von den gesetzlichen Regelungen erfasst werden sollen nach § 327 Abs. 5 BGB-E Datenträger, deren einziger Zweck die Speicherung digitaler Inhalte ist.

Es lässt sich also festhalten, dass von der Digitale-Inhalte-Richtlinie und deren nationalgesetzlicher Umsetzung all solche Produkte erfasst werden sollen, die dem Verbraucher in digitaler Form angeboten werden oder deren körperliche Form wirklich ausschließlich der Zurverfügungstellung digitaler Inhalte dient.

Der Anwendungsbereich der Richtlinie und im Ergebnis auch des Gesetzesentwurfs (§ 327 Abs. 1 BGB-E) beschränkt sich in personeller Hinsicht auf Verbraucherverträge. Geregelt wird also nur das Vertragsverhältnis zwischen Unternehmern und Verbrauchern.[4]

Herauszuheben sind in dem Gesetzesentwurf die Mangelgewährleistung und die Updatepflicht.

III.Mängelgewährleistung

Es wird im Regierungsentwurf zwischen subjektiven Mängeln, objektiven Mängeln und Integrationsmängeln unterschieden. Die Gesetzessystematik suggeriert ein Nebeneinander von subjektiven Mängeln (Abweichungen von der tatsächlich vereinbarten Beschaffenheit) und objektiven Mängeln (Abweichungen von der Beschaffenheit vergleichbarer Produkte durchschnittlicher Güte siehe § 327e BGB-E). Im Gegensatz zum herkömmlichen Vertragsrecht, in welchem die Relevanz der durchschnittlichen Beschaffenheit vergleichbarer Waren nur nachrangig Bezugspunkt für die Feststellung eines Mangels ist und vorerst die vertraglichen Vereinbarungen relevant sind, stellt ein solches Nebeneinander ein Novum dar. Wie sich diese Konstellation in der Praxis auswirkt und ob Konflikte in der Mangelzuordnung entstehen können, wird sich zeigen.

IV. Updatepflicht

Ebenfalls eine Neuheit stellt die Pflicht des Unternehmers zur Aktualisierung seines Produktes aus § 327f BGB-E dar. Während sich die Pflichten des herkömmlichen Unternehmers nach Erfüllung der vertraglichen Hauptpflicht regelmäßig auf die Gewährleistungsrechte beschränkt, trifft den Anbieter digitaler Produkte nach dem Regierungsentwurf zukünftig die Pflicht, dem Verbraucher Aktualisierungen seines Produktes und insbesondere auch Sicherheitsupdates zur Verfügung zu stellen. Diese Pflicht gilt für den gesamten Zeitraum der Bereitstellung des digitalen Produktes. § 327f Abs. 2 BGB-E normiert eine Haftungserleichterung für den Unternehmer, für den Fall, dass sich ein Produktmangel aus der fehlenden Installation einer angebotenen Aktualisierung ergibt.

Eine nunmehr nicht nur vertragliche vereinbarte, sondern auch gesetzliche Pflicht des Unternehmers zur anhaltenden Betreuung der von ihm angebotenen Produkte, wird zwangsläufig zu einer Mehrbelastung der Unternehmer führen. Ob und in welchem Umfang diese im Lichte des Verbraucherschutzes dennoch tragbar ist, wird Gegenstand zukünftiger Rechtsprechung werden.

V. Konflikt mit Urheber- und Datenschutzrecht

Durch die Digitale-Inhalte-Richtlinie werden im Ergebnis viele Regelungen über immaterielle Güter getroffen, welche ihren Schutzbereich ebenfalls im Urheberrecht finden. Nach Vorgabe in den Erwägungsgründen bleibt das Urheberrecht durch die Richtlinie „unberührt".[5] Allerdings werden sich früher oder später Konfliktbereiche der beiden Regelungsfelder ergeben. Exemplarisch sei hier die Verkehrsfähigkeit digitaler Werkexemplare genannt. In den letzten Jahren wurde viel darüber diskutiert, inwiefern einmal erworbene digitale Güter (Software, E-Books) auf einem Gebrauchtmarkt weiter veräußert werden

4 Spindler/Sein in MMR 2019, 415, 116.

5 ErwGr. 36 RL (EU) 2019/770

dürfen. Dabei spielen vor allem auch die Rechte des Urhebers an seinem einst geschaffenen und kopierten Werk eine große Rolle. Während bzgl. des sogenannten Erschöpfungsgrundsatzes im Urheberrecht klare Linien der europäischen Rechtsprechung gezogen wurden,[6] bleibt abzuwarten, wie diese Grundsätze sich auf beispielsweise den Rechtsmangelbegriff in der Praxis der Verbraucherverträge über digitale Produkte auswirken werden.

Art. 3 Abs. 1 UAbs. 2 DID-RL eröffnet die Möglichkeit, auch personenbezogene Daten als Gegenleistung für die Bereitstellung digitaler Produkte einzusetzen. So könnte beispielsweise die Bereitstellung eines Musik-Streamingdienstes gegen Mitteilung personenbezogener Daten des Verbrauchers erfolgen. Diese können für den Dienstleister gewinnbringend für Werbezwecke analysiert und verarbeitet werden. Problematisch wird hier die Vereinbarkeit mit dem europäischem Datenschutzrecht und der abwehrrechtlichen Konzeption der Datenschutz-Grundverordnung sein.[7]

VI. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Auch Hochschulen und wissenschaftliche Einrichtungen sind von der Richtlinie betroffen. Durch jene werden teilweise digitale Produkte angeboten oder vermittelt.[8] Die Beschäftigten kommen auch in der Rolle des Verbrauchers mit den Angeboten in Berührung. Die praktische Bearbeitung und Klärung der aufgeworfenen Problematiken wird gerade mit Blick auf die Relevanz digitaler Produkte für den zukünftigen Vertragsalltag große Bedeutung im deutschen und europäischen Zivilrecht haben.

6 siehe auch Gielen, Bis hierher und nicht weiter, DFN-Infobrief Recht 5/2020.

7 Sattler in NJW 2020, 3623, 3627.

8 Nach Art. 2 Nr. 5 DID-RL können auch öffentliche juristische Personen Unternehmer sein.

Digital Services Act: Das Plattformgrundgesetz?

Die Europäische Union gegen die Meinungsmacht der Plattformen

von Nico Gielen

Zwei Jahrzehnte hat die Europäische Union der Entstehung großer Online-Plattformen zugesehen und dabei tatkräftig mitgeholfen. Nun wird eine Kehrtwende eingeleitet. Zu viel Hass, zu viel Desinformation, zu viel Verbrauchertäuschung – all dies möchte die Union mit dem Digital Services Act (DSA) bekämpfen. Ein Mittel hierzu soll auch ein Datenzugang für Forscher sein.

I. Einleitung

Es stellt keine Neuigkeit dar, dass auf Online-Plattformen, die paradoxerweise auch als soziale Netzwerke bezeichnet werden, kein Blatt vor den Mund genommen wird – es wird gelogen, betrogen und gehetzt. Spinner, Betrüger und Hetzer können sich dort leicht zu Netzwerken verbünden und geschützt von einer Filterblase, wahlweise alternative Fakten oder Hasstiraden selbstbewusst in die Welt hinaustragen. Die sozialen Netzwerke helfen dabei: Sie bilden ein Megafon für Verschwörungstheoretiker, einen Pranger für Mobbingopfer und das wohl effektivste Propagandamittel der Geschichte.

Zwanzig Jahre hat sich die Europäische Union dies nicht nur angesehen, sondern ihre schützende Hand über dieses System gehalten. Seite an Seite mit den USA erließ sie eine Haftungsprivilegierung für Hosting-Diensteanbieter – die Amerikaner in Section (Sec.) 230 Communication Decency Act und die Europäer in Art. 14 E-Commerce-Richtlinie (-RL). Damit waren und sind Betreiber von Plattformen im Grundsatz nicht für das verantwortlich, was in ihren Netzwerken geschieht. Erst wenn ihnen angetragen wird, auf ihrer Plattform geschehe Illegales, müssen sie dies überprüfen. Es ist kein Zufall, dass im Anschluss hieran Facebook (2004), YouTube (2005) und Twitter (2006) gegründet wurden; das Haftungsprivileg – das nicht umsonst als die Magna Charta des Internets geführt wird – hat es möglich gemacht. Abgesehen von einzelnen Ausnahmen, ist die Europäische Union diesen Kurs bis heute weitergefahren.

Das brachte einzelne Mitgliedstaaten dazu, die immer größer werdende Regulierungslücke selbst zu füllen. So erließen Frankreich Loi Avia, Deutschland das Netzwerkdurchsetzungsgesetz (NetzDG) und Österreich das Kommunikationsplattform-Gesetz (KoPl-G) Gesetze, welche die Meinungsmacht der großen Plattformen einzuhegen versuchten. Ihnen ist gemein, dass sie die sozialen Netzwerke verpflichten wollten, rechtswidrige Inhalte innerhalb einer bestimmten Frist zu löschen. Frankreich war dabei etwas überambitioniert und verpflichtete zur Löschung innerhalb nur einer Stunde – der Verfassungsrat kassierte das Gesetz wenige Wochen später wegen Verstoßes gegen die Meinungsfreiheit (Conseil Constitutionel, Entscheidung vom 18.6.2020, Az. 2020-801 DC). Auch in Deutschland wurden Stimmen laut, wonach das NetzDG sowohl mit der Verfassung als auch mit dem Unionsrecht nur schwerlich in Einklang zu bringen sei. Die Zweifel bestanden aber nicht nur in rechtlicher Hinsicht. Auch wurde bezweifelt, ob der verfolgte Zweck mit den Gesetzen überhaupt erreicht werden kann. So beurteilen Plattformen die Inhalte auch heute noch primär nach ihren eigenen Nutzungsbedingungen und werfen erst im zweiten Schritt ihren Blick auf das nationale Recht. Im Übrigen ist auch bei den Kernproblemen – Hass und Desinformation – kein Rückgang zu verzeichnen. Der Sturm auf das Kapitol in den USA hat dies nochmal schmerzlich verdeutlicht.

Der deutsche Gesetzeber entschied sich aufgrund der schleppenden Fortschritte für einen weiteren Einzelgang. Ein Hate-Speech-Gesetz müsse her und dazu ein Gesetz zur Änderung des NetzDG. Das eine soll die Plattformen verpflichten, schwere Straftaten an das BKA zu melden und das andere die

Meldung von rechtswidrigen Inhalten erleichtern sowie den Rechtsschutz betroffener Nutzer verbessern. Die Offensive des Gesetzgebers schaffte es jedoch noch nicht einmal am Bundespräsidenten vorbei, der insbesondere die Meldepflicht für offensichtlich verfassungswidrig hielt und seine Unterschrift verweigerte. Darum startete die große Koalition einen Rettungsversuch mit einem „Reparaturgesetz", das reparieren soll, was es noch gar nicht gibt und dem Hate-Speech-Gesetz mit aller Gewalt über die Latte der Verfassungswidrigkeit verhelfen soll.

II. Digital Services Act – Ein Überblick

Die kläglichen Versuche der nationalen Gesetzgeber, die den Binnenmarkt zu fragmentieren drohten, konnte sich dann auch die Europäische Union nicht mehr ansehen. Deswegen veröffentlichte sie Ende 2020 einen Entwurf des DSA, der als Verordnung die nationalen Regelungen obsolet machen würde.

Der DSA behält zwar die Haftungsprivilegierung bei, unterwirft die Plattformen aber umfangreichen Sorgfaltspflichten. Dabei knüpft er an den Begriff des rechtswidrigen Inhalts an und erfasst damit alle Inhalte, die gegen das Recht eines Mitgliedstaats oder der Europäischen Union verstoßen, unabhängig davon, was dieses Gesetz zum Gegenstand hat (Art. 2 lit. g DSA). Erfasst werden alle Diensteanbieter, die auch von der E-Commerce-RL erfasst wurden, nur wächst das Pflichtenprogramm des DSA mit der Größe der Plattform. So sind kleinste und kleine Unternehmen von vielen Pflichten ausgenommen (Art. 13 Abs. 2, 16 DSA), wohingegen sehr große Plattformen, deren monatliche Nutzerzahl sich auf mindestens 45 Mio. Personen beläuft (Art. 25 DSA), den umfangreichsten Pflichten unterliegen.

Ein Anliegen des DSA ist es, dass Dienstanbieter ihren Nutzern eine benutzerfreundliche Möglichkeit bieten müssen, rechtswidrige Inhalte zu melden (Art. 14 DSA). Exakte Bearbeitungsfristen sind jedoch nicht vorgesehen, nur „zeitnah" solle man vorgehen. Des Weiteren soll der Rechtsschutz derjenigen Nutzer verbessert werden, die von Löschungen oder Sperrungen der Plattform betroffen sind. Dafür sollen ein internes Beschwerdesystem (Art. 17 DSA) und außergerichtliche Streitbeilegungsstellen (Art. 18 DSA) geschaffen werden. Eine weitere Säule des DSA stellen umfangreiche Transparenzpflichten dar, sei es durch ausführliche Transparenzberichte, Erläuterungen in den Allgemeinen Geschäftsbedingungen oder Aufklärung über Werbung gegenüber dem Verbraucher. Sehr große Online-Plattformen sollen darüber hinaus die systemischen Risiken, die von ihnen ausgehen, bewerten und versuchen, diese zu mindern (Art. 26 f. DSA).

Zuletzt bietet der DSA ein neues Durchsetzungsregime. Es sollen neue Behörden – sog. Koordinatoren für digitale Dienste – eingerichtet werden und die Europäische Kommission wird mit weitgehenden Befugnissen ausgestattet. Zum Beispiel soll es ihr möglich sein, im Falle der Untätigkeit eines Mitgliedstaates das Ruder an sich zu reißen. Dann kann sie auch Bußgelder bis maximal 6 Prozent eines Jahresumsatzes verhängen (Art. 59 DSA). Damit soll dem Missstand abgeholfen werden, dass sich die großen Plattformen vorwiegend im überforderten Irland niederlassen, um einer Kontrolle zu entgehen.

III. Insbesondere: Datenzugang für Forscher

In dem Bündel von Transparenzmaßnahmen befindet sich auch Art. 31 Abs. 2 DSA, wonach Forschern ein Zugang zu den Daten sehr großer Online-Plattformen verschafft werden soll. Dafür soll die Kommission oder der Koordinator für digitale Dienste ein entsprechendes Zugangsverlangen an die jeweilige Plattform richten dürfen. Die Forscher sollen mithilfe dieser Daten Forschungsarbeiten erstellen, die etwa zum Verständnis der systemischen Risiken dieser Plattformen beitragen. Aber auch Daten zur Funktionsweise von eingesetzten Algorithmen und der Umgang mit Beschwerden sollen mögliche Untersuchungsgegenstände darstellen (ErwGr. 64). Der Zugang soll nicht jedem, sondern nur zugelassenen Forschern zur Verfügung stehen. Eine Zulassung setzt voraus, dass der Forscher mit einer akademischen Einrichtung verbunden und von gewerblichen Interessen unabhängig ist sowie über einschlägige Sachkenntnis verfügt (Art. 31 Abs. 4 DSA).

Darüber hinaus darf der Datenzugang nur unter Berücksichtigung der Interessen der Online-Plattformen und der Nutzer erfolgen. Deswegen muss der Forscher sich zur Einhaltung von Vertraulichkeit und Datensicherheit verpflichten (Art. 31 Abs. 4 DSA). Außerdem soll die Kommission diese Punkte in delegierten Rechtsakten, welche die technischen Bedingungen und die Zwecke des Zugangs konkretisieren sollen,

berücksichtigen (Art. 31 Abs. 5 DSA). Es ist nicht unwahrscheinlich, dass gerade Datensicherheit und Vertraulichkeit für Diskussionen sorgen werden, ob im Einzelfall ein Datenzugang erfolgen kann. So hat die Online-Plattform auch das Recht, ein Zugangsverlangen mit Verweis auf die Sicherheit ihres Dienstes oder den Schutz ihrer Geschäftsgeheimnisse abzulehnen (Art. 31 Abs. 6 lit. b DSA). Die Vorschrift sieht allerdings nicht vor, dass die Online-Plattform diese Verweigerung sonderlich begründen müsste. Sie muss nur einen Vorschlag für einen alternativen Zugang zu den angeforderten oder anderen geeigneten Daten unterbreiten. Der Koordinator für digitale Dienste oder die Kommission beschließt schließlich, ob dem Alternativvorschlag stattgegeben wird (Art. 31 Abs. 7 DSA). Wenn die Online-Plattform aber ihre Verweigerung nicht begründen muss, ist zweifelhaft, auf welcher Grundlage man der Verweigerung entgegentreten möchte. Somit wird es entscheidend sein, dass der Geheimnisschutz nicht als Vorwand genutzt wird, den Zugang zu versperren.

IV. Fazit

Der Digital Services Act wird die Probleme des Internets sicherlich nicht auf einen Schlag lösen, aber er kann einen ersten Schritt darstellen, die Wirkungsweise und die systemischen Risiken von Online-Plattformen besser zu verstehen und in der Folge auch gezielter regulieren zu können. Ein Datenzugang für Forscher kann hierbei einen wichtigen Baustein bilden. Der Erfolg eines Datenzugangs wird letztlich davon abhängen, ob der Interessenkonflikt zwischen den wissbegierigen Forschern einerseits und den auf Vertraulichkeit pochenden Plattformen andererseits angemessen aufgelöst werden kann. Insbesondere muss sichergestellt sein, dass die Ausnahmebestimmungen nicht genutzt werden können, um das begrüßenswerte Ziel der Vorschrift zu torpedieren.

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