NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

DFN infobrief recht

8 / 2022
August 2022

Die Pfeife tönt zur Nachspielzeit

BMJ legt Referentenentwurf für Hinweisgeberschutzgesetz vor

Hausfriedensbruch goes digital

Der Bundesrat legt dem Bundestag einen neuen Gesetzesentwurf zum digitalen Hausfriedensbruch vor

Alea iacta est: Uploadfilter bleiben

Die Entscheidung des EuGH über die Europarechtskonformität von Uploadfiltern

Kurzbeitrag: Strenger geht's immer!

EuGH: Strengere Gesetze zum Kündigungsschutz von Datenschutzbeauftragten widersprechen nicht der DSGVO

Die Pfeife tönt zur Nachspielzeit

BMJ legt Referentenentwurf für Hinweisgeberschutzgesetz vor

von Justin Rennert

Das Bundesministerium der Justiz (BMJ) hat den Referentenentwurf eines Hinweisgeberschutzgesetzes vorgelegt.[1] Dieses dient der Umsetzung einer EU-Richtlinie, die längst hätte in nationales Recht gegossen werden müssen. Das Gesetz soll Whistleblower besser vor Repressalien schützen, wenn sie Informationen über Rechtsverstöße im eigenen Betrieb melden oder an die Öffentlichkeit weitergeben. Der Gesetzesentwurf erfasst auch Hochschulen unmittelbar.

I. Einleitung

Die Europäische Union möchte Whistleblower besser vor Repressalien schützen. Deshalb hat sie bereits im Jahre 2019 die „Richtlinie zum Schutze von Personen, die Verstöße gegen das Unionsrecht melden" erlassen (RL (EU) 2019/137). Doch EU-Richtlinien gelten in den Mitgliedsstaaten nicht unmittelbar, sondern müssen erst durch die nationalen Gesetzgeber in nationales Recht umgesetzt werden. Im September 2021 berichteten wir im DFN-Infobrief Recht erstmals über das deutsche Gesetzgebungsverfahren zu einem Umsetzungsgesetz für die EU-Whistleblowerrichtlinie.[2] Die Umsetzungsfrist für die Richtlinie lief schließlich schon am 17. Dezember 2021 ab. Zwar hatte das Bundesjustizministerium im letzten Jahr bereits einen ersten Referentenentwurf vorgelegt. Auf diesen konnten sich SPD und CDU allerdings seinerzeit nicht verständigen. Die Bundesrepublik verfehlte also die Frist zur Umsetzung. Um möglichst zügig Konformität mit dem EU-Recht herzustellen, hat jetzt das nunmehr FDP-geführte Justizressort einen neuen Referentenentwurf vorgelegt. Der vorliegende Beitrag stellt die wichtigsten Komponenten dieses Referentenentwurfes vor.

II. Die Verpflichtung zur Einrichtung von Meldestellen

Kernstück des Gesetzesentwurfes ist die Verpflichtung zur Einrichtung von internen Meldestellen für jeden Beschäftigungsgeber. Das bedeutet konkret: Ist das Gesetz einmal in Kraft, so muss jeder Arbeitgeber eine interne Meldestelle einrichten, an die sich Beschäftigte wenden können, wenn sie beabsichtigen, Rechtsverstöße zu melden. Das Gesetz unterscheidet dabei nicht zwischen öffentlich-rechtlich und privatrechtlich organisierten Beschäftigungsgebern. Die Verpflichtung zur Errichtung einer Meldestelle trifft demnach auch staatliche Institutionen, mithin auch Hochschulen in staatlicher Trägerschaft. Einzige Einschränkung: Die Pflicht zur Einrichtung einer internen Meldestelle gilt nur für Beschäftigungsgeber und Organisationseinheiten mit jeweils in der Regel mindestens 50 Beschäftigten.

Die interne Meldestelle kann aus einer oder mehreren bei dem jeweiligen Beschäftigungsgeber bereits tätigen Personen bestehen. Der Beschäftigungsgeber kann allerdings auch einen Dritten mit der Wahrnehmung dieser Aufgabe betrauen (das Contracting ist also ähnlich wie bei externen Datenschutzbeauftragten möglich). Die bei der Meldestelle tätigen Personen dürfen zwar für ihren Beschäftigungsgeber weiterhin andere Tätigkeiten ausüben, der Beschäftigungsgeber hat aber sicherzustellen, dass dies nicht zu Interessekonflikten führt.

---

1 Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Hinweisgeberschutz.pdf - zuletzt abgerufen am 05.07.2022

2 Rennert, „Meinungsfreiheit verpflichtet" in: DFN-Infobrief Recht 09/2021.

Ist die interne Meldestelle einmal eingerichtet, muss der Beschäftigungsgeber Meldekanäle einrichten, über welche die Beschäftigten die Meldestelle erreichen können. Interessant ist hierbei, dass explizit keine Verpflichtung besteht, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen. Wer es als Beschäftigungsgeber ernst meint mit dem Hinweisgeberschutz, der wird aber wohl dennoch Kanäle für eine anonyme Übermittlung errichten.

Sobald der Beschäftigte die Meldung abgegeben hat, muss die Meldestelle die Meldung prüfen und mit der hinweisgebenden Person Kontakt halten. Nach dieser Prüfung kann sich die Meldestelle entscheiden, Folgemaßnahmen zu ergreifen. Sie hat insbesondere die Befugnis, interne Untersuchungen bei dem Beschäftigungsgeber durchzuführen. Auch hier zeigt sich wieder, dass die Umsetzung des Gesetzes vom guten Willen des jeweiligen Beschäftigungsgebers abhängt. Denn wie effektiv die internen Untersuchungen der Meldestelle sind, entscheidet nicht zuletzt deren personelle Besetzung und die Anzahl der dort tätigen Personen. Alternativ kann die Meldestelle das Verfahren an eine zuständige Behörde zwecks weiterer Untersuchungen abgeben. Hierzu zählen unter anderem die Staatsanwaltschaften. Doch der Gesetzesentwurf sieht nicht nur die Einrichtung interner Meldestellen vor. Er regelt darüber hinaus die Einrichtung externer, staatlicher Meldestellen beim Bund und bei den Ländern. Der Bund ist verpflichtet, beim Bundesamt für Justiz eine externe Meldestelle einzurichten. Die Länder können optional eigene externe Meldestellen errichten, bei denen Personen Meldungen betreffend die Landes- oder Kommunalverwaltung abgeben können.

Auch die externen Meldestellen müssen wiederum Meldekanäle bereitstellen. Die Befugnisse der externen Meldestellen unterscheiden sich leicht von denen der internen Meldestellen. Externe Meldestellen können nach pflichtgemäßem Ermessen, den betroffenen Beschäftigungsgeber kontaktieren. Harte Eingriffsbefugnisse räumt der Entwurf der externen Meldestelle jedoch nicht ein. Sie ist hier wiederum auf die Kooperation mit anderen Behörden, insbesondere Strafverfolgungs- und Gefahrenabwehrbehörden angewiesen. An diese Behörden kann sie die gesammelten Informationen jederzeit weitergeben.

III. Schutzmaßnahmen für Hinweisgeber

Der Gesetzesentwurf möchte Hinweisgebern nicht nur eine einfache Möglichkeit geben, Verstöße zu melden. Er möchte auch erreichen, dass Hinweisgeber umfassend vor Repressalien geschützt sind, wenn sie sich einmal dazu durchgerungen haben, eine Meldung abzugeben. Die zweite Säule, auf der das Hinweisgeberschutzgesetz aufbaut, besteht daher aus mehreren Schutzmaßnahmen für Hinweisgeber. Hierzu gehören: das Verbot von Repressalien sowie eine Beweislastumkehr bei Benachteiligungen im Beruf sowie ein Schadensersatzanspruch. Der Begriff der „Reperessalien“ ist dabei denkbar weit gefasst. Hierunter fallen alle Handlungen oder Unterlassungen im Zusammenhang mit einer beruflichen Tätigkeit, die eine Reaktion auf eine Meldung oder eine Offenlegung sind und durch die der hinweisgebenden Person ein ungerechtfertigter Nachteil entsteht. Denn nicht immer greift der Arbeitgeber direkt zu harten arbeitsrechtlichen Maßnahmen. Häufig sind Repressalien objektiv nicht leicht zu erfassen und Beschäftigte haben unter ihnen eher unterschwellig zu leiden. Hier lässt sich beispielsweise an die Nichtberücksichtigung eines Beschäftigten für ein wichtiges Projekt denken oder die Zuweisung eines neuen, kleineren Büros. Wichtigstes Merkmal einer Repressalie ist die Kausalität zwischen der Meldung des Verstoßes und dem ungerechtfertigten Nachteil für den Beschäftigten.

Doch die Kausalität wird ein Beschäftigter vor Gericht häufig nicht beweisen können. Deswegen sieht der Gesetzesentwurf eine Beweislastumkehr vor: Erleidet eine hinweisgebende Person nach der Meldung eines Verstoßes einen Nachteil im Zusammenhang mit der beruflichen Tätigkeit, so haben die Gerichte zu vermuten, dass es sich um eine Repressalie handelt. Der Beschäftigungsgeber müsste vor Gericht dann wiederum erst einmal das Gegenteil beweisen, dass also gerade keine Kausalität zwischen dem Hinweis und der Benachteiligung bestand. Zu den typischen Repressalien gehören: die Versagung der Teilnahme an Weiterbildungsmaßnahmen, die Herabstufung oder Versagung einer Beförderung, Aufgabenverlagerung, Gehaltsminderung, oder die Nichtumwandlung eines befristeten Arbeitsvertrages in einen unbefristeten.

Der Gesetzesentwurf versucht Beschäftigte nun auf die folgende Weise vor solchen oder ähnlichen Maßnahmen zu schützen: Zunächst sieht er die rechtliche Nichtigkeit der Repressalie vor, sofern es sich dabei um ein Rechtsgeschäft handelt. Unter die rechtsgeschäftlichen Repressalien fallen zum Beispiel die

Kündigung oder die Gehaltsminderung. Der Beschäftigte profitiert von dieser Schutzmaßnahme beispielsweise in einem Kündigungsschutzprozess. In Kombination mit der Beweislastumkehr für Repressalien kann er sich so relativ leicht gegen eine Kündigung zur Wehr setzen.

Der Gesetzesentwurf räumt dem Beschäftigten schließlich auch einen Schadensersatzanspruch ein. Danach muss der Verursacher der Repressalie dem Hinweisgeber den aus der Repressalie entstehenden Schaden ersetzen. Zu den typischen Schäden im Nachgang erlittener Repressalien gehört zum Beispiel der entgangene Mehrverdienst aus einer unterbliebenen Gehaltserhöhung.

Der Gesetzesentwurf setzt jedoch nicht nur auf private Durchsetzung der Beschäftigtenrechte. Er ermächtigt auch Behörden, gegen Behinderungen von Hinweisgebern vorzugehen. Deshalb enthält er abschließend einige Bußgeldvorschriften, die von den Verwaltungsbehörden durchgesetzt werden können. Demnach handelt derjenige ordnungswidrig und kann in der Folge mit Bußgeld bedacht werden, der eine Repressalie vornimmt. Zudem erklärt es der Gesetzesentwurf zur Ordnungswidrigkeit, wenn ein Beschäftigungsgeber nach Inkrafttreten des Gesetzes keine interne Meldestelle einrichtet und betreibt. Auch die Beschäftigten können schließlich mit Bußgeld belegt werden: und zwar dann, wenn sie vorsätzlich eine unrichtige Information offenlegen.

IV. Sorgfaltspflichten der Hinweisgeber

Hinweisgeber müssen sich jedoch auch an gewisse Regeln halten. Dies ist im europäischen Recht seit Langem anerkannt. So hat der Europäische Gerichtshof für Menschenrechte sich in mehreren Entscheidungen bereits dazu geäußert, welche Sorgfaltspflichten Whistleblower zu beachten haben, wenn sie planen, einen Rechtsverstoß zu melden oder offenzulegen.[3] Auch der Referentenentwurf nimmt dieses Konzept auf und sieht Sorgfaltspflichten vor, die Hinweisgeber unbedingt zu beachten haben.

Grundsätzlich bestehen für Hinweisgeber zwei Sorgfaltspflichten: Die wichtigste Sorgfaltspflicht ist die Pflicht zur Prüfung auf den Wahrheitsgehalt. Hinweisgeber müssen vor der Meldung jedenfalls Grund zu der Annahme haben, dass die jeweilige Information der Wahrheit entspricht. Die zweite Sorgfaltspflicht ist die Pflicht zur Meldung.
Standardmäßig sind Hinweisgeber verpflichtet, den Rechtsverstoß bei einer oben beschriebenen internen oder externen Meldestelle zur Kenntnis zu bringen. Nur, wenn sie eine dieser Stellen wählen, fallen sie unter den Schutz des Gesetzes. Für Meldungen leuchtet dies freilich noch ein. Anders behandelt der Gesetzesentwurf jedoch Offenlegungen von Informationen. Ein Hinweisgeber legt eine Information dann offen, wenn er der Öffentlichkeit Informationen über Verstöße zugänglich macht. Dies kann zum Beispiel die Weitergabe an einen Presseverlag oder einen Fernsehsender sein, aber auch die Veröffentlichung in einem eigenen Internetblog. Vor derartigen Offenlegungen haben Hinweisgeber schärfere Sorgfaltspflichten zu beachten. Hinweisgeber müssen sich hier vor der Offenlegung an eine externe Meldestelle wenden, also eine solche, die der Staat selbst betreibt. Der Weg über die externe Meldestelle darf nur entfallen in Fällen äußerster Dringlichkeit oder wenn im Falle einer externen Meldung Repressalien oder die Unterdrückung von Beweismitteln zu befürchten sind.

Dieses Regelungskonzept mutet seltsam an. Der Gesetzesentwurf verschafft rechtlichen Schutz im Austausch gegen staatliche Beteiligung am Kommunikationsprozess. Die Sorgfaltspflicht zur externen Meldung berührt die Kommunikationsfreiheiten sowohl von Hinweisgebern als auch von Zeitungs- und Fernsehredaktionen. Haben sich Hinweisgeber einmal dazu durchgerungen, an die Öffentlichkeit zu gehen, so müssen sie gemäß dem Gesetzesentwurf direkt auch den Staat beteiligen. Auf der anderen Seite wissen Redaktionen nun, dass der Staat in der Regel vorinformiert ist, wenn sie eine Enthüllungsgeschichte abdrucken oder ausstrahlen wollen. Darin liegt eine nicht unerhebliche Beeinträchtigung der Presse- und Meinungsfreiheit. Es bleibt abzuwarten, ob das Konzept im weiteren Gesetzgebungsverfahren unverändert bleibt.

V. Fazit und Bedeutung für Hochschulen

Tritt das Gesetz einmal in Kraft, so bedeutet das für Hochschulen und Forschungseinrichtungen konkreten Handlungsbedarf. Sie müssen eine interne Meldestelle betreiben, an die sich Hinweisgeberinnen und Hinweisgeber mit Informationen über Rechtsverstöße wenden können. Die Einrichtung der Meldestelle

3 Ausführlich zur Rechtsprechung des EGMR: Rennert, „Meinungsfreiheit verpflichtet“ in: DFN-Infobrief Recht 09/2021.

obliegt für staatlich betriebene Hochschulen allerdings der obersten Bundes- oder Landesbehörde, mithin regelmäßig den Wissenschaftsministerien. Innerhalb eines Bundeslandes sollen sich mehrere Hochschulen optional auch eine zentrale Meldestelle teilen können.

Insgesamt ist der Gesetzesentwurf zu begrüßen. Die EU und der nationale Gesetzgeber verschärfen damit ihre Aktivitäten zum Schutz von Individuen, die einen Beitrag zum öffentlichen Meinungsbildungsprozess leisten. Änderungsbedarf gibt es allerdings noch im Rahmen der Sorgfaltspflichten vor Offenlegung einer Information. Die Sorgfaltspflicht zur externen Meldung ist ein zu gravierender Eingriff in die Kommunikationsfreiheiten von Hinweisgebern und Redaktionen.

Wann der Bundestag das Gesetz verabschieden kann, kann gegenwärtig nicht gesagt werden. Es handelt sich bislang lediglich um einen Referentenentwurf. Dieser befindet sich derzeit in der kabinettsinternen Beratung der Bundesregierung. Erst nach einer Einigung innerhalb der Bundesregierung kann er zum Regierungsentwurf werden und von den koalitionstragenden Fraktionen in das Parlament eingebracht werden.

Hausfriedensbruch goes digital

Der Bundesrat legt dem Bundestag einen neuen Gesetzesentwurf zum digitalen Hausfriedensbruch vor

von Nicolas John

Kriminalität macht bekanntermaßen auch im Internet keinen Halt. Schon jetzt sind Hasskommentare oder Drohungen in sozialen Netzwerken allgegenwärtig. Doch nicht nur Taten gegen die persönliche Ehre nehmen im digitalen Raum weiter zu, sondern auch Angriffe gegen Einrichtungen werden immer häufiger wahrgenommen. So sind sog. „Distributed-Denial-of-Service-Angriffe" (DDoS-Angriffe) oder „Verschlüsselungstrojaner" auch für IT-Laien keine unbekannten Begriffe mehr. Aufgrund dieser Entwicklungen legte der Bundesrat dem Bundestag einen Gesetzesentwurf zur Strafbarkeit des digitalen Hausfriedensbruchs vor.

I. Hintergrund

Im Mai 2022 hat eine Recherche von Jan Böhmermann ans Licht gebracht, dass Delikte im Internet wie Beleidigung, das Verwenden von Kennzeichen verfassungswidriger und terroristischer Organisationen oder Volksverhetzung bei den Ermittlungsbehörden oftmals ins Leere führen.[1] Die Gründe hierfür waren vielfältig. Nicht nur die Ermittlungsbehörden zeigten teilweise wenig Interesse an der Verfolgung der Straftaten, auch das Ausfindigmachen der Täter:innen stellte sich oftmals als Herausforderung dar. Doch während die Delikte der Recherche unter existierende Straftatbestände des Strafgesetzbuchs (StGB) fallen, sind auch digitale Handlungen denkbar, welche einen Schaden verursachen, nicht aber unter Strafe stehen.
So stellt es sich nach der Auffassung der Hessischen Landesregierung zum Beispiel bei DDoS-Angriffen oder bei Angriffen mit Verschlüsselungstrojanern dar.

DDoS-Angriffe haben das Ziel, die Erreichbarkeit eines Internetdiensts oder Servers zu stören, um damit einen möglichst großen Schaden anzurichten.[2] Die Angreifenden bedienen sich hierfür eines großen ferngesteuerten Netzwerks aus verschiedenen Computern. Diese lassen sie gleichzeitig auf den angegriffenen Internetdienst oder Server zugreifen. Auf diese Art schaffen die Angreifenden eine künstliche Überlastungssituation und der angegriffene Dienst baut sich als Ergebnis des Angriffs nur langsam auf oder ist gar nicht mehr zu erreichen.
Dieses ferngesteuerte Netzwerk aus vielen Computern wird auch Botnetz genannt. Um ein solches Botnetz zu schaffen, bedienen sich die Angreifenden oftmals fremder Computer. Damit diese ferngesteuert werden können, infizieren sie die jeweiligen Computer mit einer Schadsoftware und übernehmen so unbemerkt die Kontrolle über die Geräte. Je mehr Computer die sog. Botmaster hierbei als Botnetz zusammenschalten, desto schlagkräftiger werden die Angriffe. So bestehen die größten bekannten Botnetze aus weit mehr als 100.000 Einzelgeräten. Der bisher stärkste Angriff hatte ein Datenverkehraufkommen von über 3,47 Terabit/s.[3]

Angriffe mit Verschlüsselungstrojanern verfolgen ein anderes Ziel: Die Angreifenden schleusen für die Attacke zunächst eine Schadsoftware in ein bestehendes Netzwerk ein. Sobald die Software im Netzwerk auf einem oder mehreren Geräten platziert ist, fängt diese an, alle vorhandenen Daten zu verschlüsseln. Ein

1 Böhmermann, Magazin Royale-Ausgabe vom 27.05.2022, abrufbar unter https://tatütata.fail (zuletzt abgerufen am 28.06.2022).

2 Zu den Diensten des DOS-Schutzes des DFN-Vereins s. Gröper/Kahl, IT-Sicherheit reloaded – Security Operations im DFN.

3 Heise, Microsoft kontert Rekord-DDoS-Attacke mit 3,47 Terabit auf Cloud-Plattform Azure, https://www.heise.de/news/Microsoft-kontert-Rekord-DDoS-Attacke-mit-3-47-Terabit-auf-Cloud-Plattform-Azure-6341800.html (zuletzt aufgerufen am 28.06.2022).

bekanntes Beispiel hierfür sind die Emotet-Angriffe.[4] Hierbei verleiteten Angriff-E-Mails, welche täuschend echt den E-Mails von bekannten Absendenden entsprachen, zum Download einer Software. Die Empfangenden waren im Glauben, ein normales Dokument oder Programm herunterzuladen. Durch diese heruntergeladene Schadsoftware war es den Angreifenden aber möglich geworden, entsprechende Verschlüsselungstrojaner (z. B. Ryuk) auf Computer im angegriffenen Netzwerk zu installieren. Durch die Verschlüsselung der Daten war es den Nutzenden des Netzwerks nicht mehr möglich, auf die im Netzwerk gespeicherten Informationen zuzugreifen. Der Zugriff war nur mit einem entsprechenden Schlüssel möglich. Diese Situation wurde von den Angreifenden meist für eine Erpressung ausgenutzt. Sie verlangten ein Lösegeld und gaben im Gegenzug zur Zahlung den benötigten Schlüssel frei.
Doch damit die Angreifenden überhaupt die Schadsoftware auf den Geräten installiert bekommen, verschicken sie im Vorfeld oftmals massenhaft E-Mails, welche im Anhang oder als Link die Schadsoftware enthalten. Um die abertausenden Spam-Mails versenden zu können, bedienen sich die Angreifenden auch hier Botnetzen, welche wie oben beschrieben mittels fremder Computer aufgespannt werden.

II. Auffassung der Hessischen Landesregierung und des Bundesrats

Aufgrund dieser Entwicklungen sieht die Hessische Landesregierung gesetzgeberischen Handlungsbedarf im Strafrecht. [5] Nach der Auffassung des Hessischen Landtags decken die jetzt schon geltenden §§ 202a, 303a und 303b StGB die Übergriffe der Angreifenden auf die fremden Computer zum Zweck des Botnetzes strafrechtlich nicht ausreichend ab.

§ 202a StGB stellt das Ausspähen von Daten unter Strafe. Dies ist dann der Fall, wenn sich jemand unbefugten Zugang zu Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind und wenn der Zugang unter Überwindung der Zugangssicherung geschieht. § 303a StGB pönalisiert unter dem Tatbestand der Datenveränderung die rechtswidrige Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten. Und § 303b StGB sieht als Computersabotage das Stören einer Datenverarbeitung, welche für einen anderen von besonderer Bedeutung ist als strafbar an, wenn dies z.B. dadurch geschieht, dass eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird.

In den Erwägungen des Gesetzesentwurfs weist der Bundesrat darauf hin, dass z.B. Daten von § 202a StGB nur dann geschützt seien, wenn für den unberechtigten Zugriff auf die Daten eine besondere Zugangssicherung überwunden werde. Wenn für diese Überwindung aber kein erheblicher technischer oder zeitlicher Aufwand erforderlich ist, sei der Tatbestand nicht erfüllt. Dies könne z.B. dann der Fall sein, wenn dem Angreifenden erforderliche Passwörter schon bekannt sind.
Auch der Schutz des § 303a StGB sei dann nicht gegeben, wenn die Schadsoftware keine Veränderungen an den Daten vornimmt. Die derzeitige Technologie lasse sog. Hardwaretrojaner schon zu. In solchen Fällen sei eine nicht hinzunehmende Schutzlücke vorhanden.
Und zwar falle die Durchführung von DDoS-Angriffen unter den Tatbestand des § 303b StGB, jedoch würde jeder sonstige Eingriff, der nicht mit einer Störung der Datenverarbeitung einhergeht, nicht erfasst werden.
Darüber hinaus bemängelte der Bundesrat in seinen Erwägungen, dass sich nach geltendem Recht die Begehung einer Computertat oftmals nicht nachweisen lasse, da sich die Schadsoftware nach ihrer Ausführung oder bei ihrer Entdeckung häufig selbst lösche.

Diese verschiedenen Erwägungen brachten den Bundesrat dazu, dem Bundestag nun einen Gesetzesentwurf zum „Digitalen Hausfriedensbruch“ zur Abstimmung vorzulegen.[6] Dabei ist dieser Vorschlag nicht der erste seiner Art. Schon 2016 und 2018 schlug der Bundesrat aufgrund hessischer Initiative einen wortgleichen § 202e StGB E vor. Die beiden Vorschläge wurden in den jeweiligen Legislaturperioden nicht weiterverfolgt und für erledigt erklärt.

4 Zu den Emotet-Angriffen Uphues, Der Feind in meinem Netz – Teil 1, DFN-Infobrief Recht 1/2020; Uphues, der Feind in meinem Netz – Teil 2, DFN-Infobrief Recht 2/2020.

5 Der Gesetzesentwurf findet sich im Wortlaut mit Begründung in: BT-Drs. 20/1530.

6 Pressemitteilung des Deutschen Bundestages vom 02.05.2022, https://www.bundestag.de/presse/hib/kurzmeldungen-892402 (zuletzt abgerufen am 28.06.2022).

III. Der Gesetzesentwurf zum digitalen Hausfriedensbruch

Der Gesetzesentwurf des Bundesrates verfolgt das Ziel, die Rechtsgedanken des „Hausfriedenbruchs“ aus § 123 StGB und des „unbefugten Gebrauch eines Fahrzeugs“ aus § 248b StGB in die digitale Welt zu übertragen und zu der Schaffung eines neuen § 202e StGB E führen. Die Erforderlichkeit der Erweiterung der Straftatbestände begründet er auch anhand der Rechtsprechung des Bundesverfassungsgerichts (BVerfG), welches 2008 in einem Urteil zur Onlinedurchsuchung das „Computergrundrecht“ festgestellt hatte.[7] Der neue § 202e StGB E soll dieses Grundrecht weiter stärken. § 202e StGB E stellt damit die „unbefugte Benutzung informationstechnischer Systeme“ unter Strafe, um existierende Strafbarkeitslücken zu schließen. Digitale Angriffe jeglicher Art sollen mit dem vorgeschlagenen Tatbestand umfasst werden, insbesondere auch die Benutzung fremder Computersysteme zum Zwecke von Cyberangriffen.

Nach Abs. 1 des Entwurfs soll der Tatbestand dann erfüllt sein, wenn der Angreifende unbefugt entweder sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft, es in Gebrauch nimmt oder einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem solchen System beeinflusst oder in Gang setzt. Für die Erfüllung des Tatbestandes muss kein Erfolg eintreten, es genügt die reine Tathandlung. Allerdings muss die Handlung geeignet sein, berechtigte Interessen eines anderen zu beeinträchtigen. Darüber hinaus sieht der neue § 202e StGB E auch strafverschärfende Tatbestände vor. Diese knüpfen teilweise an objektive Umstände an, z.B. ob die Tat gegen ein Entgelt vorgenommen wird oder ob die Tat als Bande begangen wird. Im Übrigen knüpfen sie an subjektive Umstände an, wie z.B. die Absicht des Angreifenden, sich oder einen Dritten zu bereichern oder die Absicht, eine Gefahr für die öffentliche Sicherheit herbeizuführen. Insbesondere für die Absicht, einen Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken, lässt der neue § 202e Abs. 4 StGB E eine Freiheitsstrafe von bis zu 10 Jahren zu. Zu diesen Infrastrukturen gehören vor allem Einrichtungen der Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung oder des Finanz- und Versicherungswesens.[8]

IV. Kritik

Der Entwurf ist bislang auf wenig Gegenliebe gestoßen. Die Kritik wird dabei nicht nur von der Bundesregierung in einer Stellungnahme geübt, sondern auch in der juristischen Fachwelt.[9] Die Inhalte der Kritiken lassen sich in vier Kernthemen zusammenfassen: Es gebe keine Regelungslücke, der Tatbestand des neuen § 202e StGB E sei zu weit gefasst, es gebe keine Praxisrelevanz für die neue Norm und die Rechtsprechung des BVerfG zum Computergrundrecht sei nicht richtig interpretiert worden und tauge daher nicht zur Begründung.

1. Keine Regelungslücke

Die Kritiker:innen sind sich einig, dass die vom Bundesrat gesehene Regelungslücke zumindest nicht in dem dargestellten Ausmaß existiert. Denn schon das Programmieren einer Schadsoftware, welche die Errichtung eines Botnetzes ermöglichen soll, falle unter § 202c StGB, der Vorbereitung des Ausspähens und Abfangens von Daten. Außerdem falle nach Ansicht der Bundesregierung der Aufbau eines Botnetzes regelmäßig entgegen der Auffassung des Bundesrates unter den Tatbestand des § 202a StGB, dem Ausspähen von Daten.
Darüber hinaus sei § 303a StGB einschlägig, soweit die Schadsoftware Daten verändere. Insbesondere sei es nicht haltbar, dass § 303a StGB nicht einschlägig sei, wenn dem System schlicht neue Daten hinzugefügt werden. Denn unabhängig davon, wann das Hinzufügen neuer Dateien ein Verändern von Dateien darstellen kann (so ist das Hinzufügen neuer Dateien in einem Unix-basierten Betriebssystem wohl immer eine Veränderung der Dateien), müssen für das Funktionieren eines Botnetzes

7 BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07 u.a., ECLI:DE:BVerfG:2008:rs20080227.1bvr037007.

8 Zu den kritischen Infrastrukturen informiert das BSI auf seiner Webseite ausführlich unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (zuletzt aufgerufen am 28.06.2022).

9 Die Kritiken sind unter nachfolgen Quellen nachzulesen: Stellungnahme der Bundesregierung, BT-Drs. 20/1530, S. 19; Buermeyer, „Digitaler Hausfriedensbruch“: IT-Strafrecht auf Abwegen, https://www.lto.de/recht/hintergruende/h/entwurf-straftatbestand-digitaler-hausfriedensbruch-botnetze-internet/ (zuletzt abgerufen am 28.06.2022); Johannsen, Der digitale Hausfriedensbruch nach § 202e StGB E – braucht es die „Lex-Botnetz“?, abrufbar unter http://rechtundnetz.com/digitaler-hausfriedensbruch/ (zuletzt abgerufen am 28.06.2022); Mavany, ZRP 2016, 221.

Ressourcen des infiltrierten Systems zugewiesen werden. Hierzu sind die entsprechenden Protokolle anzupassen, wodurch es zu einer Veränderung von Daten i.S.d. § 303a StGB komme. Auch die Herstellung und das Verstecken der Internetverbindung zum Botmaster setze die Veränderung von Programmen voraus. DDoS-Angriffe mit Hilfe von ferngesteuerten Botnetzen fielen außerdem sowieso schon unter den Tatbestand der Computersabotage gem. § 303b StGB.

2. Zu weit gefasster Tatbestand

Neben dem mangelndem Regelungsbedürfnis rügen die Kritiker:innen auch die vorgeschlagene Weite des neuen Tatbestandes. Es drohe die Pönalisierung von Alltagsverhalten. Während das unbefugte Einschalten eines nicht durch ein Passwort gesicherten Smartphones nach dem neuen § 202e StGB E schon eine Straftat darstellen würde, gibt es in der analogen Welt keine vergleichbare Strafbarkeit. Denn z. B. das unbefugte Aufschlagen eines Notizbuchs bliebe straflos. Das Erfordernis der Überwindung eines Zugangsmechanismus für die Strafbarkeit erscheine daher nach wie vor sachgerecht, die angeführten Schwierigkeiten beim Nachweis der Zugangssicherung können die Begründung einer solchen Strafbarkeit nicht ersetzen.
Auch würde z. B. das Einwählen in ein ungesichertes WLAN den Straftatbestand der neuen Norm erfüllen. Ob sich die einwählende Person am Ende strafbar macht oder nicht, hinge allein vom Einverständnis des Betreibenden ab. Die Bagatellklausel des Paragrafen („Beeinträchtigung berechtigter Interessen eines andern“) sei dagegen zu abstrakt, um diese Sachverhalte rechtssicher einzugrenzen.

3. Keine Praxisrelevanz

Die neue Regelung des § 202e StGB E habe keine Auswirkungen auf die Praxis. Denn während wie eben aufgezeigt Alltagsverhalten plötzlich strafbar sein könnte, sei kaum ersichtlich, wie der neue Tatbestand zur Verfolgung von tatsächlich strafwürdigem Verhalten beitragen soll. Das Errichten und Betreiben von Botnetzen finde stets im Geheimen statt. Die Ermittlungsbehörden erlangen daher meistens von der Tatbestandsverwirklichung keine Kenntnis. Und selbst wenn ein Botnetz aufgedeckt werden könne, seien die Botmaster selten zu ermitteln und befänden sich fast immer im Ausland.

Zudem sei die Verfolgung von Botmastern wie oben schon dargestellt mangels Strafbarkeitslücke durch andere Normen sichergestellt, es gebe daher keinen Bedarf für die neue Norm. Insbesondere bei einem Sachverhalt, in welchem das Botnetz zu einem kriminellen Zweck eingesetzt wird, wie z. B. bei Verschlüsselungstrojanern, griffen meist Straftatbestände, welche ein höheres Strafmaß vorsehen, wie z.B. die Erpressung nach § 253 Abs. 1 StGB.

4. Falsche Auslegung der Rechtsprechung des BVerfG

In seiner Begründung zum Entwurf führt der Bundesrat die Stärkung des vom BVerfG festgestellten „Computergrundrechts“ an. Es sei die Aufgabe des Strafrechts, einen lückenlosen Schutz des Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen. Daher entnimmt der Bundesrat diesem Urteil, dass das ausschließliche Gebrauchsrecht an IT-Geräten schützenswert sei.
Doch diese Auffassung wird ebenfalls kritisiert. Denn das „Computergrundrecht“ schütze nicht das ausschließliche Gebrauchsrecht an einem informationstechnischen System, sondern es schütze den Zugriff Dritter auf die von IT-Systemen verarbeiteten Daten. Es gehe in dem Urteil somit um eine Form des vorgezogenen Datenschutzes. Die IT-Systeme selbst sollen durch das Grundrecht nicht geschützt sein. Der Bundesrat interpretiere das Urteil daher falsch. Darüber hinaus lehne das BVerfG in dieser Entscheidung letztendlich eine Verletzung der Unverletzlichkeit der Wohnung nach Art. 13 Grundgesetz (GG) ab. Den „digitalen Hausfriedensbruch“ mit den Rechtsgedanken der §§ 123, 248b StGB begründen zu wollen, liege daher fern.

V. Fazit und Bedeutung für Hochschulen und Forschungseinrichtungen

Wie es mit dem Entwurf nun weitergeht, ist vorerst offen. Die Kritik an den vergangenen Entwürfen hatte den Bundesrat offensichtlich nicht zu Änderungen veranlasst. So bleibt es jetzt Sache des Bundestages, einen Beschluss über den Entwurf zu fassen. Ob der Entwurf hierfür nochmals angepasst wird, bleibt abzuwarten. Die Bundesregierung erkennt das Ziel des Vorschlags, Botnetz-Kriminalität zu bekämpfen, in jedem Fall an und beabsichtigt die Prüfung des Erfordernisses einer Überarbeitung des Computerstrafrechts im Austausch mit Wissenschaft und Praxis.

In jedem Fall sind die Entwicklungen zu beobachten. Denn auch die informationstechnischen Systeme von Hochschulen und Forschungseinrichtungen unterliegen dem Schutzbereich des vorgeschlagenen Tatbestandes. Die meisten Einrichtungen haben in der Vergangenheit Erfahrungen mit digitalen Angriffen verschiedener Art gemacht. Die Ausweitung der Strafbarkeit würde also auch unmittelbar für Angriffe gegen Hochschulen und Forschungseinrichtungen Relevanz haben. Insbesondere dann, wenn von den Angriffen kritische Infrastrukturen wie Universitätskliniken betroffen sind. Doch ob ein neuer Tatbestand im StGB am Ende tatsächlich die Angreifenden zur Strecke bringt, bleibt weiter fraglich.

Alea iacta est: Uploadfilter bleiben

Die Entscheidung des EuGH über die Europarechtskonformität von Uploadfiltern

von Johanna Schaller

Der Europäische Gerichtshof (EuGH) weist die von Polen erhobene Klage gegen Art. 17 der Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt (DSM Richtlinie) ab und schafft so Rechtssicherheit für die umstrittenen Verpflichtungen und die Haftung von Internetdiensteanbietern beim Upload von Inhalten.

I. Hintergrund der Entscheidung

Die Debatte um die sogenannten Upload-Filter ist nicht neu.[1] Die Reform des Urheberrechts durch die DSM Richtlinie der EU aus 2019 sollte primär dazu dienen das Urheberrecht zu modernisieren und Urhebern für ihre Inhalte im Netz eine bessere Vergütung zu sichern. In Deutschland und anderen EU-Ländern löste dies, insbesondere die Einführung der Uploadfilter, große Diskussionen und Proteste aus. Unter Uploadfiltern werden allgemeinhin automatisierte Computerprogramme verstanden, die Daten vor deren Veröffentlichung oder Hochladen nach dezidierten Kriterien kontrollieren und sortieren.
Nun hat sich der EuGH im Rahmen einer Klage des Mitgliedstaats Polen vor allem mit der Frage befasst, ob eine faktische Verpflichtung von Internetdiensteanbietern zur Verwendung dieser Uploadfilter durch europäisches Sekundärrecht mit dem europäischen Grundrecht auf freie Meinungsäußerung und Informationsfreiheit aus Art. 11 der EU-Grundrechte-Charta (GRCh) vereinbar ist.

Konkret geht es dabei um den umstrittenen Artikel 17 der DSM Richtlinie. Dieser sieht in Abs. 4 Buchstabe b und c vor, dass Diensteanbieter hochgeladene Inhalte zuvor auf Verstöße gegen das Urheberrecht überprüfen müssen, um sich nicht selbst für diese haftbar zu machen.
Angesichts der unübersehbaren Mengen an zu überprüfenden Daten, werden die Diensteanbieter de facto verpflichtet, Prüfsysteme zu verwenden, die eine vorherige automatische Filterung der Inhalte gewährleisten, also die umstrittenen Uploadfilter zu implementieren.

Dies stieß in weiten Teilen der Gesellschaft auf Kritik dahingehend, dass durch eine derartige „Vorabkontrolle" die freie Meinungsäußerung und die Informationsfreiheit gefährdet würde. Auch die Republik Polen erblickte in der Haftungsfreistellung mit Beweislast beim Diensteanbieter, die durch Art. 17 Abs. 4 Buchstabe b und c der DSM Richtlinie statuiert wird, einen Verstoß gegen die Grundrechte der freien Meinungsäußerung und Informationsfreiheit des Art. 11 der GRCh und erhob im Mai 2019 Klage vor dem EuGH auf Nichtigerklärung der Vorschrift. Im Detail beantragte Polen die Nichtigerklärung des Art. 17 Abs. 4 Buchstabe b und c DSM Richtlinie. Hilfsweise zielte der Antrag darauf ab, die gesamte Vorschrift des Art. 17 für nichtig zu erklären.

II. Die Entscheidung des EuGH

Mit Urteil vom 26. April 2022[2] entschied der EuGH, dass die Regelung des Art. 17 DSM Richtlinie und die damit verbundene Vorabkontrolle die Meinungsfreiheit und die Informationsfreiheit der Nutzer zwar einschränke, die Regelung jedoch insgesamt verhältnismäßig sei.
Das Europäische Parlament, das durch Frankreich und die Kommission unterstützt wurde, brachte gegen den Antrag vor,

1 Tiessen, Anfang vom Ende?, DFN-Infobrief Recht 01/2019; Gielen, First Rule: Do not talk about Uploadfilter, DFN Infobrief Recht 01/2020; Rennert, Habemus Reform, DFN Infobrief Recht 07/2022.

2 https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.

dieser sei bereits nicht zulässig, da sich die Buchstaben b und c des Abs. 4 des Artikels 17 nicht vom Rest des Artikels trennen ließen. Die von Polen als Klägerin angestrebte nur teilweise Nichtigerklärung eines Unionsrechtsakts sei nur dann möglich, wenn der für nichtig erachtete Teil auch rechtlich vom Rest des Rechtsakts trennbar ist. Dies sei aber dann nicht der Fall, wenn die teilweise Nichtigerklärung zur Folge hätte, dass der Wesensgehalt des Rechtsakts durch den Wegfall des nunmehr für nichtig erklärten Teils verändert wird.
Unter Verweis auf die Folge einer Veränderung des Wesensgehalts verneinte auch der EuGH die Trennbarkeit des Art. 17 DSM Richtlinie. Die Bestimmungen des Art. 17 bilden nach der Auffassung des Gerichtshofs eine Einheit und zielten darauf ab, ein Gleichgewicht zwischen den Rechten und Interessen der Anbieter, denen der Nutzer ihrer Dienste und denen der Rechteinhaber herzustellen. Dagegen lasse sich die Regelung des Art. 17 von den übrigen Regelungen der Richtlinie trennen, sodass der Hilfsantrag der Republik Polen auf Nichtigerklärung von Art. 17 DSM Richtlinie insgesamt demzufolge zulässig ist.
Sodann befasste sich der EuGH in dem Urteil mit der hoch umstrittenen Frage, ob Art. 17 einen Verstoß gegen das Grundrecht auf freie Meinungsäußerung und Informationsfreiheit aus Art. 11 GRCh darstelle. Polen rügte in dem vorgebrachten Antrag einen schwerwiegenden Eingriff, der den Wesensgehalt des Grundrechts missachte und unverhältnismäßig sei.

1. Vorliegen eines Eingriffs

Das Grundrecht auf Meinungsfreiheit schützt die positive und negative Freiheit, eine Meinung zu äußern oder auf eine bestimmte Weise zu verbreiten.

Die Informationsfreiheit schützt den gesamten Informationsprozess, vom Empfang einer allgemein zugänglichen Information, über die Weitergabe, bis zur Speicherung und Anschaffung von Anlagen zur Entgegennahme der Information.

Polen legte in seiner Klage dar, der Eingriff in diese Rechte liege darin, dass die faktische Verpflichtung zur vorbeugenden Kontrolle sämtlicher Inhalte die Gefahr berge, dass rechtmäßige Inhalte blockiert würden und es dadurch schon gar nicht zu einer von Art. 11 GRCh geschützten Verbreitung der Inhalte kommen könnte. Ferner sei dieser Eingriff als unvermeidbare und vorhersehbare Konsequenz der Regelung in Art. 17 auch dem Unionsgesetzgeber zuzurechnen.

In seiner Entscheidung erkannte auch der EuGH einen solchen Eingriff sowie die Verantwortung des Unionsgesetzgebers an.

2. Rechtfertigung des Eingriffs

Einschränkungen eines Grundrechts können nur dann vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Zudem muss eine Regelung, die einen Eingriff enthält, klare und präzise Regeln für die Tragweite und Anwendung der betreffenden Maßnahme vorsehen.
Als legitime Zielsetzung der Regelung des Art. 17 DSM Richtlinie nennt der EuGH den Schutz der Inhaber von Urheberrechten und verwandten Schutzrechten. Diese sind als Rechte des geistigen Eigentums in Art. 17 Abs. 2 GRCh festgeschrieben und genießen so ebenfalls den Rang eines Unionsgrundrechts.
Ferner verweist der EuGH in seiner Entscheidung darauf, dass die Art. 17 Abs. 7 bis 9 der Richtlinie sowie die Erwägungsgründe 66 und 70 zu diesen Normen eine hinreichende Präzisierung derjenigen Maßnahmen bieten würden, die zur Umsetzung der faktischen Uploadfilter-Pflicht verlangt werden können. Beispielsweise sieht Art. 17 Abs. 8 sowie Erwägungsgrund 66 vor, dass die Mitgliedstaaten keine allgemeine Pflicht zur Überwachung einführen sollen und hinsichtlich der Frage, ob der Diensteanbieter die Kontrollpflichten nach Art. 17 Abs. 4 Buchstabe b und c vorgenommen hat, stets eine einzelfallbezogene Betrachtung vorzunehmen ist.

Art. 17 Abs. 7 und Erwägungsgrund 70 sehen vor, dass Inhalte, die von Nutzern generiert wurden, zu Zwecken des Zitierens, der Kritik, Rezension, Karikatur, Parodie oder Pastiche hochgeladen werden dürfen. Damit werde auch dem hohen Rang der Meinungsäußerungsfreiheit Rechnung getragen.
Darüber hinaus trete eine Haftung der Diensteanbieter für die Veröffentlichung urheberrechtswidriger Inhalte nur unter der Voraussetzung ein, dass der betreffende Rechteinhaber dem Anbieter die einschlägigen und notwendigen Informationen über diese Inhalte übermittelt. Ohne diese werden die Diensteanbieter auch nicht dazu veranlasst, dafür zu sorgen, dass die betreffenden Inhalte nicht verfügbar sind.

Der EuGH kommt so zu dem Ergebnis, dass das Recht der freien Meinungsäußerung und Informationsfreiheit aus Art. 11 GRCh nicht in unverhältnismäßiger Weise von Art. 17 Abs. 4 betroffen

sei. Der Unionsgesetzgeber habe klare Grenzen gezogen, um zu verhindern, dass rechtmäßige Inhalte beim Hochladen gefiltert und gesperrt werden. Insbesondere stelle die Regelung des Art. 17 DSM Richtlinie konkret dar, dass ein Filtersystem, das nicht hinreichend zwischen einem unzulässigen Inhalt und einem zulässigen Inhalt unterscheidet mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit unvereinbar sei. Bei der Ausgestaltung der Filtersysteme selbst komme es sodann auf die Umsetzung durch die Mitgliedstaaten an.
Es sei also „Sache der Mitgliedstaaten, bei der Umsetzung von Art. 17 der Richtlinie in ihr innerstaatliches Recht darauf zu achten, dass sie sich auf eine Auslegung dieser Bestimmung stützen, die es erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Charta geschützten Grundrechten sicherzustellen“, so der EuGH in der Pressemitteilung.

III. Fazit / Bedeutung für Hochschulen

Das Urteil nimmt die Mitgliedstaaten der EU in die Pflicht, bei Umsetzung von Art. 17 der DSM Richtlinie den angemessenen Ausgleich zwischen Beeinträchtigung der Meinungs- und Informationsfreiheit und Schutz des geistigen Eigentums zu wahren. In Deutschland werden die europäischen Vorgaben durch das UrhDaG umgesetzt. Da das Urteil die Vorgaben der DSM Richtlinie gerade nicht beanstandet, besteht auch kein Änderungsbedarf im Folgenden für das UrhDaG.

Auch für Hochschulen bleibt folglich alles wie seit der Urheberrechtsreform gehabt.

Anders als die Regelungen der DSM Richtlinie zum Text und Data-Mining und zu nicht verfügbaren Werken, betreffen die Verpflichtungen aus Art. 17 DSM Richtlinie die Hochschulen und Forschungseinrichtungen, wie jeden Internetnutzer, nur mittelbar.[3] Das Bedürfnis zur Verwendung von Uploadfiltern besteht grundsätzlich nur dann, wenn der Online-Inhaltedienst mit dem Hauptzweck betrieben wird, eine große Menge an von Dritten hochgeladenen urheberrechtlich geschützten Inhalten zu speichern und öffentlich zugänglich zu machen, diese mit Gewinnerzielungsabsicht bewerben und mit anderen Online-Inhaltediensten um dieselbe Zielgruppe konkurrieren (vgl. § 2 UrhDaG).

Sofern Hochschulen selbst Upload-Plattformen betreiben (beispielsweise ein universitätseigenes Videoportal, auf dem Studierende Inhalte hochladen können) sind sie gem. Art. 2 Nr. 6 der DSM Richtlinie und der Umsetzung in § 3 Nr. 2 UrhDaG von den Verpflichtungen der DSM Richtlinie ausgenommen. Nach dieser Regelung sind nicht gewinnorientierte bildungsbezogene oder wissenschaftliche Repositorien nicht von dem Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten erfasst.

Gleichwohl sind sie wie jeder andere Internetnutzer von den Regelungen im praktischen Umgang mit dem Internet betroffen. Gerade im Hinblick auf die zunehmende Digitalisierung an Hochschulen und die Heranziehung von sozialen Netzwerken und Online-Inhaltediensten, wie beispielsweise durch Nutzung der Plattform „YouTube“ zu Zwecken der Öffentlichkeitsarbeit oder auch der Lehre und Vermittlung von Wissen, ist eine Auseinandersetzung mit der Entwicklung der Umsetzung der Uploadfilter in angemessenem Ausgleich zur Meinungs- und Informationsfreiheit aber durchaus von Interesse und weiter zu beobachten.

3 Gielen, First Rule: Do not talk about Uploadfilter, DFN Infobrief Recht 01/2020; Rennert, Habemus Reform, DFN Infobrief Recht 07/2022.

Kurzbeitrag: Strenger geht's immer!

EuGH: Strengere Gesetze zum Kündigungsschutz von Datenschutzbeauftragten widersprechen nicht der DSGVO

von Nicolas John

Der Gerichtshof der Europäischen Union (EuGH) entschied jüngst mit Urteil vom 22. Juni 2022 (Az.: C-543/20), dass die Datenschutz-Grundverordnung (DSGVO) strengere Gesetze eines Mitgliedstaates bei arbeitgeberseitiger Kündigung eines betrieblichen Datenschutzbeauftragten nicht verbiete. Der Vorabentscheidung des EuGHs liegt ein Verfahren aus Deutschland zugrunde.

I. Hintergrund

Der Entscheidung des EuGHs geht ein Rechtsstreit vor dem Bundesarbeitsgericht (BAG) voraus. Eine Mitarbeiterin war ordentlich wegen einer Unternehmensumstrukturierung aus betriebsbedingten Gründen gekündigt worden. Zuvor war sie als Datenschutzbeauftragte des Unternehmens bestellt worden. Im Rahmen der unternehmerischen Umstrukturierung sollte die Stelle des Datenschutzbeauftragten zukünftig eine externe Person wahrnehmen. Die Arbeitnehmerin erhob hierauf Kündigungsschutzklage und berief sich vorrangig auf ihren Sonderkündigungsschutz aus § 38 Abs. 2 i.V.m. § 6 Abs. 4 S. 2 Bundesdatenschutzgesetz (BDSG). Dieser Sonderkündigungsschutz erlaubt eine Kündigung von Beschäftigten, welche als Datenschutzbeauftragte fungieren, nur bei Vorliegen eines wichtigen Grundes. Dieser lag ihrer Auffassung nach mit der Umstrukturierung nicht vor, die Kündigung sei daher unwirksam. Die Instanzgerichte[1] überzeugte diese Argumentation und hielten die Kündigung der Arbeitnehmerin für unwirksam.

Schlussendlich gelangte die Klage der Arbeitnehmerin vor das BAG. Dieses meldete Zweifel an, ob die Vorgaben des BDSG mit den Vorschriften der DSGVO vereinbar seien.

Nach Art. 38 Abs. 3 S. 2 DSGVO darf die Person des Datenschutzbeauftragten „wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden". Diese Regelung ist damit weniger restriktiv als die Vorgaben des BDSG, welches die ordentliche Kündigung eines Arbeitnehmenden, welche:r zum Datenschutzbeauftragten ernannt worden ist, gänzlich ausschließt. Lediglich eine Kündigung aus wichtigem Grund ist zulässig. Die DSGVO sieht diese Beschränkung in ihrer Formulierung nicht vor, sodass hiernach etwa die betriebsbedingte Kündigung aufgrund einer Umstrukturierung zumindest nicht explizit ausgeschlossen ist. Normalerweise genießt die DSGVO gegenüber nationalem Recht Anwendungsvorrang. Insoweit können nationale Rechtsvorschriften wie das BDSG nicht angewendet werden, wenn sie den Vorgaben der DSGVO widersprechen. Die von der DSGVO abweichende, strengere Regelung des BDSG veranlasste das BAG daher, den EuGH zur Klärung anzurufen. Mit seiner Vorlagefrage wollte das BAG nun klären, ob die Vorgaben der DSGVO überhaupt strengere nationale Regelungen zulassen.

II. Die Entscheidung des EuGH

Der EuGH entschied auf die Vorlage des BAG nun, dass Art. 38 Abs. 3 S. 2 DSGVO dahingehend auszulegen sei, dass die strengeren Normen des BDSG der DSGVO nicht entgegenstehen und die Regelungen somit wirksam sind.
Der EuGH begründet seine Entscheidung unter Auslegung des Art. 38 DSGVO. Demnach bezwecke dieser allein die Sicherstellung der funktionellen Unabhängigkeit der Datenschutzbeauftragten. Die Norm schütze Datenschutzbeauftragte vor negativen Entscheidungen des Arbeitgebenden, die in Zusammenhang der Erfüllung ihrer Aufgaben stehen.

1 Arbeitsrechtliche Klagen müssen zunächst vor dem Arbeitsgericht erhoben werden. Soweit gegen das Urteil des Arbeitsgerichts ein Rechtsmittel eingelegt wird, kommt es zur Verhandlung vor der nächsthöheren Instanz.

Kein Ziel der Vorgaben des Art. 38 Abs. 3 S. 2 DSGVO sei es dagegen, das Arbeitsverhältnis insgesamt zwischen dem Verarbeitenden und dessen Beschäftigten zu regeln. Vielmehr sei das Verhältnis allenfalls beiläufig betroffen. Außerdem gehe es bei Art. 38 DSGVO weder um den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten noch um den freien Datenverkehr, sondern um Sozialpolitik. Im Bereich der Sozialpolitik habe die Union und ihre Mitgliedstaaten eine geteilte Zuständigkeit, weshalb es den Mitgliedsstaaten freisteht, strengere Vorschriften hierzu zu erlassen. Wichtig sei nur, dass diese dem Unionsrecht und insbesondere den Bestimmungen der DSGVO nicht widersprechen.
Bei den streitgegenständlichen Vorgaben des BDSG sei dies nach Ansicht des EuGHs nicht der Fall.

III. Bedeutung für Hochschulen und Forschungseinrichtungen

Das Urteil stärkt die unabhängige Position von Datenschutzbeauftragten. Auch wenn die meisten Hochschulen nicht an die Vorgaben des BDSG sondern die Vorschriften der jeweiligen Landesdatenschutzgesetz (LDSG) beachten müssen, lässt sich diese Rechtsprechung des EuGHs auf diese Normen übernehmen. Soweit sich ähnliche Vorgaben zum Kündigungsschutz von Datenschutzbeauftragten in den LDSGs finden, ist auch bei diesen davon auszugehen, dass sie wirksam sind und nicht den Vorgaben der DSGVO widersprechen.

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

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn