Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

3 / 2023
März 2023

AI-mazing: DALL-E und ChatGPT malen ein Bild der Zukunft

Überblick zu den rechtlichen Problemen bei der Verwendung von KI-Software

Daten-Blackout!

Wahrung der Rechte und Interessen Dritter bei Auskunft und Kopieherausgabeansprüchen nach der DSGVO

Schaden oder kein Schaden, das ist hier die Frage

Schlussanträge des Generalanwalts zum Ersatz immaterieller Schäden bei Datenschutzverletzungen

Karlsruhe zeigt Kante

Das Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns ist teilweise verfassungswidrig

AI-mazing: DALL-E und ChatGPT malen ein Bild der Zukunft

Überblick zu den rechtlichen Problemen bei der Verwendung von KI-Software

von Nicolas John

Künstliche Intelligenz (KI)[1] hat in der Vergangenheit vermehrt Schlagzeilen gemacht und wird immer mehr Teil unseres Alltags. Das bringt aber auch neue Herausforderungen im rechtlichen Bereich mit sich, z.B. dem Urheberrecht, Datenschutzrecht und Persönlichkeitsrecht. Während die Vorteile der KI unbestreitbar sind, müssen Fragen des Schutzes von geistigem Eigentum, der Verantwortung für automatisierte Entscheidungen und der Verbreitung unwahrer Tatsachen geklärt werden. Lösungen sind derzeit oft nur vereinzelt in Sicht. Der Beitrag soll zu den Problemstellungen daher einen ersten Überblick verschaffen.

I. Entwicklung und Einsatzgebiete von KI

Die Entwicklung Künstlicher Intelligenz (KI) ist ein schnell wachsendes Forschungsgebiet, das das Potenzial hat, viele Branchen zu revolutionieren. Die Anwendungsmöglichkeiten für KI-Software sind endlos.

Einer der wichtigsten Bereiche der KI-Forschung ist die Verarbeitung natürlicher Sprache (Natural Language Processing, NLP), bei der es um die Fähigkeit von Computern geht, menschliche Sprache zu verstehen und zu erzeugen. Die Sprachverarbeitung wird in einer Vielzahl von Anwendungen eingesetzt, z. B. in der Sprachübersetzung, der Textzusammenfassung und der Stimmungsanalyse.

Ein weiterer wichtiger Bereich der künstlichen Intelligenz ist die Bildverarbeitung, bei der es darum geht, visuelle Daten von Computern zu interpretieren und zu verstehen. Diese Technologie wird in einer Vielzahl von Anwendungen eingesetzt, darunter Bild- und Videoanalyse, Objekterkennung und Gesichtserkennung. Es wird darüber hinaus auch zunehmend bei der Überwachung, Robotik und selbstfahrenden Autos eingesetzt.

Ebenfalls ein wichtiges Einsatzgebiet von KI-Software ist das Gesundheitswesen. Medizinische Diagnose, Medikamentenentwicklung und Patientenüberwachung sind nur einige der Anwendungsfälle, für die KI zum Einsatz kommen kann. KI-gestützte Systeme helfen Ärzten und Forschern, bessere Entscheidungen zu treffen, die Ergebnisse für die Patienten zu verbessern und die Kosten im Gesundheitswesen zu senken.

Vielversprechende Nutzungsmöglichkeiten von künstlicher Intelligenz bietet schließlich das selbstfahrende Auto. KI-gestützte Systeme werden jetzt schon für Aufgaben wie die autonome Navigation und die Erkennung von Hindernissen eingesetzt. Es wird erwartet, dass selbstfahrende Autos die Sicherheit im Straßenverkehr erhöhen, Verkehrsstaus verringern und die Mobilität von Menschen, die nicht selbst fahren können, verbessern.

II. ChatGPT und DALL-E

Zwei Beispiele für solche KI-Programme sind DALL-E und ChatGPT, welche in letzter Zeit immer wieder für Schlagzeilen gesorgt haben. Doch was können diese Programme?

1 Im Englischen „Artificial Intelligence“ (AI).

ChatGPT ist ein Spracherzeugungsmodell, das maschinelle Lerntechniken zur Texterzeugung verwendet. Es wurde anhand eines umfassenden Textdatensatzes vortrainiert und ist dadurch in der Lage, einen Text so zu erzeugen, dass er der menschlichen Sprache ähnelt. Hierfür nutzt es auch den Kontext der Eingabe und die zugrundeliegende Struktur der Sprache.

Es kann für eine Vielzahl von Aufgaben der Verarbeitung natürlicher Sprache, wie z. B. Sprachübersetzung, Textzusammenfassung und Stimmungsanalyse, optimiert werden. Darüber hinaus kann es auch für Aufgaben wie die Entwicklung von Chatbots, automatisiertes Schreiben und die Erstellung von Inhalten verwendet werden.

DALL-E ist dagegen eine KI, die darauf trainiert ist, Bilder aus Texten zu erzeugen. DALL-E kann Bilder von Dingen erstellen, die es in der Realität nicht gibt, indem es die Merkmale verschiedener Bilder kombiniert. Das Modell ist in der Lage aus Textaufforderungen wie „zweibeiniger Hund fährt auf einem Skateboard“ Bilder zu erzeugen und kann so für eine Vielzahl von Anwendungen wie Spieldesign, Modedesign und Produktdesign eingesetzt werden. DALL-E wurde ebenfalls durch einen riesigen Datensatz von Bildern und Beschriftungen trainiert und kann dadurch zufallsgeneriert hochauflösende Bilder von Objekten und Szenen erzeugen, die in Textform beschrieben werden.
Die KI-Programme können Forschenden oder Entwickler:innen in verschiedenen Bereichen wie der Verarbeitung natürlicher Sprache, der Bilderzeugung und der visuellen Datenverarbeitung nützlich sein. Durch das Training mit umfangreichen Datensätzen sind sie in der Lage, qualitativ hochwertige Texte und Bilder zu generieren und sie verfügen über Feinabstimmungsfunktionen, die es Wissenschaftler:innen ermöglichen, sie für spezifische Aufgaben einzusetzen. In der Forschung können sie daher nützlich sein, wenn es darum geht, große Datenmengen zu verarbeiten, Sachverhalte selbstständig zu analysieren oder die Leistung der Modelle selbst bei verschiedenen Aufgaben zu verbessern. Der Grund, warum diese Modelle derzeit so viel Aufmerksamkeit erzeugen, ist, dass sie das Potenzial von künstlicher Intelligenz hinsichtlich des Sprachverständnisses und der Bilderzeugung für jeden zugänglich demonstrieren.[2] ChatGPT und DALL-E sind in der Lage, Aufgaben auszuführen, von denen die meisten Menschen annehmen, dass sie in erster Linie dem menschlichen Tun zuzuschreiben sind, wie z. B. das Schreiben aussagekräftiger Texte und das Erstellen von Bildern. Dies hat zu viel Aufmerksamkeit auf dem Gebiet der künstlichen Intelligenz und den möglichen Anwendungen dieser Modelle in verschiedenen Branchen geführt.

Beispiel eines KI-Erzeugnisses von „Dall-E“ nach der Eingabe „Create an oil painting of six superheroes floating in a universe full of books“

III. Rechtliche Problemstellungen

Klar ist, dass KI-Software ein großes Potenzial bietet, um Erzeugnisse verschiedenster Art zu generieren oder zu analysieren. Doch die Nutzung von KI-Software wirft in verschiedenen rechtlichen Bereichen Fragen auf, welche bislang oft nicht zweifelsfrei beantwortet werden können.

1. Urheberrecht

Das deutsche Urheberrecht wird primär durch das Urheberrechtsgesetz (UrhG) geregelt und bietet Schutz für Werke wie Literatur, Musik, Kunst und Software. Der Urheberrechtsschutz beginnt automatisch mit der Schaffung eines Werkes und bedarf keiner Registrierung. Die Inhaber des Urheberrechts haben das

2 ChatGPT kann hier ausprobiert werden: openai.com/blog/chatgpt (zuletzt aufgerufen am 27.01.2023) und Dall E hier: openai.com/dall-e-2/ (zuletzt abgerufen am 27.01.2023).

ausschließliche Recht, ihre Werke zu nutzen, zu vervielfältigen und zu verbreiten. Um ein fremdes Werk nutzen zu können, muss mit dem Urheber ein Nutzungsvertrag geschlossen werden oder eine gesetzliche Nutzungserlaubnis vorliegen, wie zum Beispiel bei einer Zitierung oder unter bestimmten Voraussetzungen zu Lehrzwecken.

Das Kernproblem stellt die Frage nach der Urheberschaft dar. Das deutsche Urheberrecht sieht vor, dass der Urheber eines Werkes die Person ist, die es geschaffen hat. Im Falle von KI-Ergebnissen kann es jedoch schwierig sein, den Urheber zu bestimmen. Einige Stimmen der Literatur argumentieren, dass KI-Erzeugnisse, die durch maschinelles Lernen und Algorithmen erstellt werden, nicht als individuelles geistiges Schaffen im Sinne des Urheberrechts gesehen werden können und daher nicht schutzfähig sind. Grund hierfür sei der Zufallsfaktor der KI. Andere Meinungen sind der Ansicht, dass KI-Software noch nicht stark genug sei. In diesem Fall sei die KI nur ein Werkzeug des Nutzenden. Es gibt auch die Auffassung, dass die Person, die das KI-Programm entwickelt hat, als Urheber angesehen werden sollte.

Wichtig ist, dass in Deutschland der urheberrechtliche Schutz von KI-generierten Werken noch nicht eindeutig bestimmt werden kann, da das Urheberrechtsgesetz keine spezifischen Bestimmungen für solche Werke enthält. Auf EU-Ebene wird jedoch über eine europaweite Anpassung der Urheberrechtsvorschriften debattiert, um den Herausforderungen zu begegnen, die neue Technologien wie KI mit sich bringen.

Aber auch die Trainingsdaten für die KI sorgen für urheberrechtliche Diskussionen. Die Frage ist, wer die Rechte an den Daten besitzt, die zum Training von KI-Programmen verwendet werden. Nach dem deutschen Urheberrecht hat der Schöpfer eines Werks das ausschließliche Recht, es zu nutzen, zu vervielfältigen und zu verbreiten.

Im Falle von KI-Lerndaten ist jedoch nicht immer klar, wer die Urheber der Daten sind und ob sie der Verwendung der Daten für das Training von KI-Programmen zugestimmt haben, weil sie oft aus einer großen Menge von Daten unterschiedlicher Quellen bestehen. Dies kann einerseits ein Problem für Unternehmen und Forschende darstellen, die die Daten für das Training ihrer KI-Programme nutzen möchten, aber nicht die erforderlichen Lizenzen einholen können. Andererseits ist bislang auch nicht abschließend geklärt, wie mit Erzeugnissen der KI umzugehen ist, wenn diese teilweise fremde Werkteile aus den Trainingsdaten enthalten.

2. Datenschutzrecht

Die Datenschutz-Grundverordnung (DSGVO) hat ebenfalls erhebliche Auswirkungen auf den Einsatz von KI-Software. Sie legt strenge Regeln für die Erhebung, Speicherung und Verwendung personenbezogener Daten fest und gilt für jede Person oder Einrichtung, die personenbezogene Daten von EU-Bürgern verarbeitet.

Eine der wichtigsten Auswirkungen der DSGVO besteht darin, dass Verantwortliche transparent darlegen müssen, wie sie personenbezogene Daten erheben und verwenden und dass sie gegebenenfalls die ausdrückliche Zustimmung von betroffenen Personen für die Verarbeitung ihrer Daten einholen müssen. Im Falle von KI-Software bedeutet dies, dass Unternehmen erklären müssen, wie und zu welchem Zweck die personenbezogenen Daten bei dieser Software verwendet werden und falls erforderlich die Zustimmung einholen.

Die DSGVO verlangt darüber hinaus, dass Verantwortliche sicherstellen, dass die von ihnen erhobenen personenbezogenen Daten richtig und aktuell sind und dass sie gelöscht oder anonymisiert werden, wenn sie nicht mehr benötigt werden. Für KI-Software bedeutet dies, dass die Daten, die zum Trainieren von Modellen verwendet werden, regelmäßig überprüft und aktualisiert werden müssen und dass die Software keine personenbezogenen Daten länger aufbewahrt, als sie benötigt werden.
Schließlich ist das Recht auf nicht automatisierte Entscheidung (Art. 22 DSGVO) ein wichtiger Aspekt, das der betroffenen Person das Recht einräumt, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht, wenn diese rechtliche Folgen für sie hat oder sie in ähnlicher Weise erheblich beeinträchtigt.

3. Persönlichkeitsrechte

Auch im Bereich der Persönlichkeitsrechte wirft die Verwendung von KI Bedenken auf. Ein zentraler Diskussionspunkt ist die Diskriminierung. Denn KI-Systeme, die auf der Grundlage voreingenommener Daten trainiert werden, können bei ihrer Entscheidungsfindung eine Diskriminierung aufrechterhalten

und sogar verstärken. Dies kann insbesondere in Bereichen wie Beschäftigung, Wohnungswesen und Kreditvergabe zu Problemen führen.

Fehlerhafte Trainingsdaten können außerdem dazu führen, dass ein KI-System falsche Informationen über Personen, z. B. einen Politiker liefert. Dies kann zu Desinformation und Misstrauen im politischen Prozess führen und möglicherweise den demokratischen Prozess beeinträchtigen.
In diesem Zusammenhang ist demnach problematisch, dass KI-Systeme bestehende gesellschaftliche Vorurteile aufrechterhalten und verstärken können und dass die Fehler in diesen Ergebnissen schwer zu erkennen und zu korrigieren sein können. Insbesondere durch die Intransparenz der Entscheidungsfindung kann es schwierig sein zu verstehen, wie eine bestimmte Entscheidung oder Schlussfolgerung entstanden ist. Hierdurch ist die Behebung von Fehlern ebenfalls erschwert.

IV. Fazit und Bedeutung für Hochschulen und Forschungseinrichtungen

Diesem Fazit ist zunächst einmal eine Klarstellung voranzustellen: Bis zu diesem Punkt wurde dieser Beitrag von einer KI auf Englisch formuliert und von einer zweiten KI anschließend ins Deutsche übersetzt. Dafür wurden verschiedene Fragen an die KI gestellt und die Antworten danach teilweise mit Übergangssätzen und Füllwörtern zu diesem Beitrag zusammengestellt. Hierdurch ist schon sichtbar, wie gut die derzeitigen KIs mittlerweile funktionieren.
Während des Prozesses haben sich aber auch oft die Grenzen der verwendeten KI gezeigt. So ist z. B. die Art der Fragestellung für das Ergebnis der KI so maßgeblich, dass bei einer unpräzisen Frage teilweise ungenaue bzw. falsche Ergebnisse erzeugt wurden. Ohne das vorhandene Fachwissen des Autors wäre dieser Beitrag nicht informativ, sondern oberflächlich und mit großer Wahrscheinlichkeit teilweise auch nicht korrekt gewesen. Dieses Problem stellt sich im Übrigen nicht nur bei juristischen Themen, generell warnen Expert:innen vor der ungeprüften Übernahme der Erzeugnisse von KIs.[3]
Dennoch werden diese Probleme in der Zukunft durch die technische Weiterentwicklung behoben werden. Die juristischen Fragestellungen sollten bis dahin allerdings geklärt werden. Denn diese betreffen auch Hochschulen und Forschungseinrichtungen. Nicht nur, dass Wissenschaftler:innen ein großes Interesse daran haben, KI-Software in verschiedensten Bereichen zu Forschungszwecken einzusetzen und hierdurch die Fragen zu klären sind, unter welchen Voraussetzungen die KI verwendet werden darf. Auch die Nutzung von KI durch Studierende stellt Hochschulen vor neue Probleme, die nicht einfach zu beantworten sind: Gilt es als Täuschungsversuch, wenn Prüflinge eine KI für die Erstellung einer Hausarbeit zu Hilfe nehmen? Liegt mit dem Verwenden eines von der KI erzeugten Textes in einer wissenschaftlichen Arbeit ein Verstoß gegen die gute wissenschaftliche Praxis vor? Gibt es eine Kennzeichnungspflicht für KI-Texte? All diese Fragen werden derzeit kontrovers diskutiert und bisher gibt es oft keine eindeutigen Antworten. Es liegt demnach in den Händen der Gesetzgeber[4], der Gerichte und der juristischen Literatur, für mehr Klarheit zu sorgen.

Erste Möglichkeiten der Klärung entwickeln sich derzeit schon. Denn verschiedene Künstler:innen und eine Plattform für Stockfotografien[5] haben in Großbritannien und den USA Klagen gegen die Macher einer KI eingereicht. Die Künstler:innen und das Unternehmen werfen den KI-Programmierern Urheberrechtsverletzungen bei der Erstellung der Trainingsdaten vor. So sollen z. B. Fotos der Stockfotoplattform ohne Zustimmung für die Trainingsdaten verwendet worden sein. In jedem Fall werden sich Verfahren dieser Art in der Zukunft häufen und zu ersten Klärungen der dringlichsten Fragen führen.

Wenn man die KI fragt, wie diese Probleme in Zukunft behoben werden können, so antwortet sie:

„Um mögliche negative Auswirkungen der KI abzumildern, sollten sich Organisationen und Einzelpersonen um die Entwicklung fairer und transparenter KI-Systeme bemühen, indem sie vielfältige und repräsentative Datensätze verwenden, diese auf Verzerrungen testen und die verwendeten Daten und Methoden transparent machen. Die rechtlichen Fragen im Zusammenhang mit KI und ihren Produkten müssen von verschiedenen Akteuren angegangen werden, darunter Regierungen, Gesetzgeber,

3 Ein Beispiel in der ZEIT: Kühl, Gut erfunden ist halb geglaubt, ZEIT online, abrufbar unter https://www.zeit.de/digital/internet/2022-12/chatgpt-kuenstliche-intelligenz-openai-chatbot (zuletzt abgerufen am 27.01.2023).

4 Zum geplanten Artificial Intelligence Act: Rennert, One KIss is all it takes, DFN-Infobrief Recht 1/2023.

5 Statement von Getty Images, abrufbar unter https://newsroom.gettyimages.com/en/getty-images/getty-images-statement (zuletzt abgerufen am 01.02.2023).

Unternehmen und Organisationen, die KI-Technologie entwickeln und nutzen.“[6]

6 Und übrigens: Auch der Titel des Beitrags stammt von der KI unter der Arbeitsaufforderung „Create a funny and humorous headline for the an article about AI like Dall-E and ChatGPT, refering to some play with words in context of a well known saying“.

Daten-Blackout!

Wahrung der Rechte und Interessen Dritter bei Auskunft und Kopieherausgabeansprüchen nach der DSGVO

von Johanna Voget

Der Auskunfts- und Kopieherausgabeanspruch des Betroffenen aus Art. 15 der Datenschutz-Grundverordnung (DSGVO) bietet in vielen Aspekten eine Bühne für rechtlichen und praktischen Diskurs. Mittelbar ist den Ansprüchen eine weitergehende datenschutzrechtliche Problematik immanent: Im Rahmen der Erfüllung der Ansprüche durch den Verantwortlichen muss auf die personenbezogenen Daten Dritter Rücksicht genommen werden, um nicht wiederum einen Verstoß gegen die Vorgaben der DSGVO durch die Verletzung der Rechte Dritter zu begründen. In diesem Infobrief soll ein Überblick über die Anforderungen an die Wahrung der Drittinteressen gegeben werden und konkrete Ausgestaltungsmöglichkeiten, wie die Schwärzung der Daten, diskutiert werden.

I. Auskunft und Kopieherausgabe nach Art. 15 DSGVO

Zur Erinnerung: In der Vergangenheit beschäftigten sich bereits mehrere DFN-Infobriefe im Rahmen des Beschäftigtendatenschutzes mit den Ansprüchen des Betroffenen auf Auskunft nach Art.15 Abs. 1 und auf Herausgabe der Datenkopien nach Art. 15 Abs. 3 DSGVO.[1] Der Auskunftsanspruch umfasst auch gesundheitsbezogene persönliche Daten, wie der Erwägungsgrund 63 zur DSGVO ausdrücklich klarstellt. Auch zu den datenschutzrechtlichen Fragen im Gesundheitskontext informierte der DFN-Infobrief zuletzt in der Ausgabe des vergangenen Monats.[2] Der Inhalt und die Reichweite der Ansprüche sind in vielen Punkten hochumstritten.[3]

Zu der Frage, wie weit der Anspruch aus Herausgabe von Datenkopien reicht, vertritt eine extensive Ansicht, dass der betroffenen Person sämtliche sie betreffenden Daten in der Rohfassung als Kopie zu übermitteln sind. Abs. 3 vermittele folglich einen eigenständigen Anspruch und werde nicht durch den Umfang des Auskunftsanspruchs nach Art. 1 begrenzt.

Dagegen spricht sich eine restriktive Ansicht dafür aus, dass Abs. 3 lediglich eine besondere Form der Auskunft darstelle, und daher nicht weitergehen könne als der Anspruch auf Auskunft.[4]

Jüngst erging eine Entscheidung des Europäischen Gerichtshofs (EuGH) (Urteil v. 12.01.2023 – C-154/21) zu der Frage, ob der Verantwortliche im Rahmen des Auskunftsanspruchs die konkrete Identität oder nur die Kategorie von Empfängern offenzulegen hat, an die er die personenbezogenen Daten des Betroffenen weitergegeben hat.

Das oberste europäische Gericht schloss sich den Ausführungen des Generalanwalts an und stellte fest, dass das Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten auch umfasst, dass der Verantwortliche, wenn diese Daten gegenüber weiteren Empfängern preisgegeben worden sind oder noch offengelegt werden, verpflichtet ist, dem Betroffenen die konkrete Identität der Empfänger mitzuteilen.

---

1 Siehe hierzu Voget, Work Data Balance: Der Beschäftigtendatenschutz, DFN-Infobrief Recht 11/2022; Gielen, 2020: Odyssee im Beschäftigtendatenschutz, DFN-Infobrief Recht 05/2021.

2 Siehe hierzu, Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

3 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Kurzpapiere/20170726_Kurzpapier_6_Auskunftsrecht.pdf?blob=publicationFile&v=6 (zuletzt abgerufen am: 01.02.2023).

4 Siehe hierzu Voget, Work Data Balance: Der Beschäftigtendatenschutz, DFN-Infobrief Recht 11/2022.

Weitestgehend unproblematisch, aber für die Betroffenen nicht minder von Relevanz sind die formalen Fragen nach den Kosten und der Form, in der die Ansprüche erfüllt werden müssen. Die Daten sind dem Betroffenen grundsätzlich in der Form, wie sie dem Verantwortlichen vorliegen, bereitzustellen. Eine Verpflichtung zur Aufbereitung und Zurverfügungstellung in einer bestimmten Form besteht mithin nicht. Art. 15 Abs. 3 S. 3 DSGVO bestimmt hierzu lediglich, dass die Auskunft und Kopien der Daten in einem gängigen elektronischen Format zu erteilen sind, wenn der Betroffene den Antrag in elektronischer Form gestellt hat, sofern sich nicht aus den Umständen etwas anderes ergibt.
In zeitlicher Hinsicht ist der Verantwortliche gem. Art. 12 Abs. 3 DSGVO verpflichtet, der betroffenen Person die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche ist in diesem Fall jedoch verpflichtet, den Betroffenen innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung zu unterrichten.
Die Auskunft ist gem. Art. 12 Abs. 5 S. 1 DSGVO grundsätzlich unentgeltlich zu erteilen. Nur in den Ausnahmefällen des Art. 12 Abs. 5 S. 2 DSGVO, bei offenkundig unbegründeten oder exzessiven, wiederholten Anträgen, kann ein Entgelt erhoben werden oder sogar eine Weigerung der Auskunftserteilung erfolgen.
Auch die erste Kopie im Rahmen des Kopieherausgabeanspruchs ist stets unentgeltlich herauszugeben. Gem. Art. 15 Abs. 3 S. 2 DSGVO kann für jede weitere Kopie sodann ein angemessenes und auf Grundlage von Verwaltungskosten zu bestimmendes Entgelt gefordert werden.

II. Schranke: Rechte und Interessen Dritter

So viel zu den Rechten des Betroffenen auf Auskunft und Herausgabe von Kopien seiner Daten gegenüber dem Verantwortlichen. In der Praxis bedeutsam sind diese Ansprüche aber nicht nur für den unmittelbar Betroffenen. Vielmehr stellt sich die Frage, welche Auswirkungen die Rechte des Betroffenen für Dritte haben, deren eigene personenbezogene Daten wiederum in den herauszugebenden Unterlagen enthalten sind. Was ist also zu beachten, wenn Dritte durch die Ansprüche des Betroffenen in ihren eigenen Rechten betroffen werden?
Wie muss mit den Daten Dritter umgegangen werden, um in Erfüllung der Ansprüche des Betroffenen keine erneute Verletzung von Vorschriften der DSGVO hervorzurufen?

Art. 15 Abs. 4 DSGVO normiert hierzu schlicht, dass das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Der Anspruch auf Kopieherausgabe wird also abstrakt durch das Verbot der Beeinträchtigung von Drittinteressen begrenzt.
Um den allgemein gehaltenen Wortlaut der Norm zu konkretisieren und für die Praxis mit Leben zu füllen, ist zunächst der Anwendungsbereich des Art. 15 Abs. 4 DSGVO zu bestimmen.
Als „andere Personen" gelten alle Personen außer der Betroffene selbst. Von dem Verbot der Beeinträchtigung sind jegliche Rechte Dritter, auch die juristischer Personen, erfasst.
In Erwägungsgrund 63 zur DSGVO findet sich eine beispielhafte Aufzählung möglicher Drittinteressen, die Geschäftsgeheimnisse oder das Recht des geistigen Eigentums, insbesondere das Recht an Software, umfasst. Handelt es sich bei den geforderten Informationen also um Geschäftsgeheimnisse des Verantwortlichen, müssen diese nicht im Rahmen des Kopieherausgabeanspruchs offengelegt werden, da insofern das Recht des Arbeitgebers „beeinträchtigt" ist.
Darüber hinaus ist auch das Geheimhaltungsinteresse von Hinweisgebern (Whistleblower) erfasst. Die Auskunft über die Identität von Hinweisgebern darf danach dann verweigert werden, wenn eine Abwägung ergibt, dass ihre Rechte gegenüber dem Informationsanspruch der betroffenen Person überwiegen.[5]
Dabei ist zu berücksichtigen, ob dem Informanten eine vertrauliche Behandlung seines Hinweises zugesichert worden ist und ob der Verantwortliche zur Aufdeckung bestimmter Normverletzungen auf solche Hinweise angewiesen ist. Dagegen hat der Informant auch bei Vorliegen einer solchen Zusicherung kein Recht auf Geheimhaltung seiner Identität, wenn hinreichende Anhaltspunkte dafür vorliegen, dass er wider besseres Wissen oder leichtfertig falsche Angaben gemacht hat.
Im Grundsatz ist jedoch bei jedem personenbezogenen Datum ein Recht des Dritten in Gestalt des Rechts auf informationelle Selbstbestimmung nach Art. 8 Grundrechte-Charta (GrCh) und Art. 2 Abs. 1 iVm Art. 1 Abs. 1 Grundgesetz (GG) betroffen. Die Auskunft kann mithin soweit verweigert werden, wie damit

5 LAG Baden-Württemberg, NZA-RR 2019, 242.

gesetzliche Verschwiegenheitspflichten verletzt werden, vgl. § 29 BDSG.[6]

Wann und ab welcher Intensität von einer Beeinträchtigung ausgegangen wird, bestimmt Abs. 4 nicht. Daher ist stets eine umfassende Prüfung und Abwägung im Einzelfall vorzunehmen, ob durch die Erfüllung des Anspruchs tatsächlich Rechte und Freiheiten Dritter betroffen sind.

Erforderlich ist eine konkrete Kollisionslage, die Besorgnis um die Gefährdung der Rechte genügt nicht. Darlegungs- und beweisbelastet ist insoweit der für die Datenverarbeitung Verantwortliche. Das Fehlen allgemeingültiger Vorgaben führt in der Praxis oftmals zu erheblicher Rechtsunsicherheit.

Darüber hinaus gilt die Schranke nach dem Wortlaut des Art. 15 Abs. 4 DSGVO nur für den Anspruch auf Kopieherausgabe nach Art. 15 Abs. 3 DSGVO.

Fraglich ist, ob eine analoge Anwendung des Abs. 4 auch auf die Abs. 1 und 2 des Art. 15 DSGVO, also auf die Auskunftserteilung und die Übermittlung von personenbezogenen Daten an internationale Organisationen oder ein Drittland, geboten ist. Ein Teil der Literatur vertritt hierzu, dass es sich um einen Redaktionsfehler des Gesetzgebers handeln müsse und nach dem Sinn und Zweck des Abs. 4 der Schutz von Drittinteressen auch bei dem Auskunftsanspruch nach Abs. 1 erforderlich ist. Dagegen wird eingewandt, dass der Gesetzgeber trotz Offenkundigkeit der Problematik nicht tätig geworden sei, es sich also nicht um eine planwidrige Regelungslücke handele und eine analoge Anwendung daher ausscheide.

III. Praktische Umsetzung: Entfernung und Schwärzung

Der Erwägungsgrund 63 zur DSGVO stellt ausdrücklich fest, dass die Schranke des Verbots der Beeinträchtigung von Drittinteressen nicht dazu führen darf, dass der betroffenen Person die Auskunft vollumfänglich verweigert wird. Sollte die Prüfung ergeben, dass durch die Kopieherausgabe Rechte oder Freiheiten Dritter beeinträchtigt werden, hat der Verantwortliche mithin die betroffenen Informationen aus der Auskunft zu entfernen, um in der Folge seiner Verpflichtung zur Herausgabe der Daten an den Betroffenen ohne datenschutzrechtlichen Verstoß gegenüber dem Dritten nachkommen zu können.

Die Entfernung der Daten kann in der Praxis bei konventioneller analoger Datenverarbeitung durch Schwärzung der Daten Dritter vor der Bereitstellung der Kopie durch den Verantwortlichen erfolgen.[7] Bei automatisierter Datenverarbeitung ist die Herstellung einer elektronischen Teilkopie möglich, wenn es sich nicht um Daten mit doppeltem oder mehrfachem Personenbezug handelt. Im Rahmen des digitalen Schwärzens von Dokumenten müssen gewisse Anforderungen erfüllt sein, um sicher zu gewährleisten, dass die geschwärzten Informationen nicht mehr lesbar sind und nicht wiederhergestellt werden können.[8]

Hierbei stellt sich im Anschluss die Frage, ob der Grund der Schwärzung angegeben werden muss, damit dies für den Betroffenen nachvollziehbar wird. Dagegen spricht der Umstand, dass der ohnehin durch Schwärzung bzw. Filterung und Entfernung der Daten bestehende Organisationsaufwand für den Verantwortlichen durch eine zusätzliche Begründungspflicht noch vergrößert wird.

IV. Bedeutung für Hochschulen

Hochschulen und Forschungseinrichtungen sind als Arbeitgeber oftmals selbst Adressaten der Ansprüche auf Auskunft und Kopieherausgabe ihrer Beschäftigten als Betroffene im datenschutzrechtlichen Sinne. Dabei ist der rechtmäßige Umgang mit Daten Dritter essentiell, um Verstöße gegen die DSGVO und damit verbundene Bußgelder bzw. Schadensersatzansprüche zu vermeiden.

Abzuwarten bleibt die nach dem Koalitionsvertrag avisierte eigenständige Ausgestaltung des Beschäftigtendatenschutzes in einem neuen Gesetz, durch die einige der rechtlichen Unsicherheiten im Rahmen des Auskunfts- und Kopieherausgabeanspruchs beseitigt werden könnten.

---

6 https://www.lda.bayern.de/media/themen/infoblatt_fuer_verantwortliche_zu_auskunft.pdf.

7 In Abgrenzung zu dem ebenfalls hochrelevanten Themenfeld der Anonymisierung von personenbezogenen Daten, instruktiv: Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023; sowie zu den Anforderungen an die Anonymisierung: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=5; https://www.dataguard.de/blog/pseudonymisierung-und-anonymisierung-in-dsgvo-und-datenschutz.

8 https://www.dpc-datenschutz.de/datenschutzkonformes-digitales-schwaerzen-von-dokumenten/; https://helpx.adobe.com/de/acrobat/using/removing-sensitive-content-pdfs.html.

Schaden oder kein Schaden, das ist hier die Frage

Schlussanträge des Generalanwalts zum Ersatz immaterieller Schäden bei Datenschutzverletzungen

von Johannes Müller

Der Generalanwalt hat sich in seinen Schlussanträgen (RS C-300/21) mit der Ersetzbarkeit von immateriellen Schäden bei Datenschutzverstößen beschäftigt. Hierbei vertritt der Generalanwalt die Auffassung, dass nicht jeder Datenschutzverstoß auch automatisch zu einem immateriellen Schaden führt. Die Voraussetzungen für das Entstehen immaterieller Schäden bedürfen daher besonderer Aufmerksamkeit.

I. Datenschutzrechtlicher Schadensersatz für immaterielle Schäden

Die Datenschutzgrundverordnung (DSGVO) sieht vor, dass Betroffene von Datenschutzverstößen sich unmittelbar gegen den für den Verstoß verantwortlichen Datenverarbeiter wehren können, indem sie von diesem Schadensersatz verlangen. Hierzu besagt Art. 82 Abs. 1 DSGVO, dass jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat.[1] Eine Besonderheit dieser Norm liegt darin, dass sie ausdrücklich besagt, dass nicht nur materielle Schäden, sondern auch immaterielle Schäden durch den Schadensersatzanspruch ersetzt werden sollen. Materielle Schäden konkret festzustellen fällt regelmäßig vergleichsweise leicht. Sie betreffen den Fall, dass einer betroffenen Person aufgrund eines Datenschutzverstoßes eine konkrete Vermögenseinbuße entsteht. Diese konkrete Vermögenseinbuße soll durch das Anerkennen eines Schadensersatzanspruches kompensiert werden. Deutlich schwieriger gestaltet sich die Frage, unter welchen Voraussetzungen durch einen Datenschutzverstoß ein immaterieller Schaden hervorgerufen wird. Würde man hierbei die Maßstäbe des deutschen Zivilrechts heranziehen, dürfte nur in Ausnahmefällen ein ersatzfähiger immaterieller Schaden anerkannt werden. Das deutsche Zivilrecht möchte immaterielle Schäden nur in engen Grenzen ersetzen (§ 253 Abs. 1 BGB), etwa bei Persönlichkeitsrechtsverletzungen oder als Schmerzensgeld.[2] Da für die Datenschutzgrundverordnung jedoch ein eigenständiger, europäischer Maßstab gilt, ist dieses enge Verständnis nicht zwingend. So fordern einige Stimmen, immaterielle Schäden gem. Art. 82 DSGVO sehr weit zu verstehen.[3] Indem bereits jedes, durch einen Datenschutzverstoß hervorgerufene, ungute Gefühl als immaterieller Schaden verstanden wird, wird Art. 82 DSGVO eine besonders bedeutsame Funktion zugewiesen. Bei einem solchen weiten Verständnis kann nahezu jeder Datenschutzverstoß, der eine natürliche Person betrifft, auch zu einem Schadensersatzanspruch führen. Verlangt man keinen konkret bestimmbaren Schaden, wird die Funktion von Art. 82 DSGVO erheblich ausgeweitet. Dann würde er nicht mehr nur dazu dienen, entstandene Einbußen zu

1 Zum datenschutzrechtlichen Schadensersatzanspruch: Uphues, Steh zu deinen Fehlern oder es kommt dir teuer zu stehen, DFN-Infobrief Recht 04/2021; Müller, Morgen Kinder werden wir klagen, DFN-Infobrief Recht 12/2022.

2 Andere Rechtsordnungen, insbesondere diejenige der USA, teilen dieses enge Verständnis von Schadensersatzansprüchen nicht. Hier ist es unter dem Begriff „Punitive damages“ deutlich weiter verbreitet, nicht ausschließlich entstandene Vermögensschäden zu ersetzen, sondern dem Schadensersatz eine sanktionierende bzw. präventive Wirkung zu verleihen.

3 So etwa Kühling/Buchner/Bergt, Datenschutzgrundverordnung BDSG Kommentar, 3. Aufl. 2020, Art. 82 DSGVO Rn. 18a f.

kompensieren, sondern auch gleichzeitig den Verantwortlichen eines Datenschutzverstoßes zu bestrafen. Ein solcher strafender Charakter eines Schadensersatzanspruchs könnte dem Datenschutzrecht eine höhere Wirksamkeit verleihen, da die meisten Datenschutzverstöße unmittelbar durch die betroffene Person sanktioniert werden könnten und nicht erst das Einschreiten einer Aufsichtsbehörde erfordern würden. Gleichzeitig wären hiermit aber auch erhebliche finanzielle Risiken für Datenverarbeiter verbunden, da Datenschutzverstöße zu zahlreichen Klagen führen könnten. Die finale Entscheidung über den Begriff der immateriellen Schäden obliegt dem Europäischen Gerichtshof (EuGH). Hierzu liegen ihm mehrere Vorlagefragen vor.[4] Zu einer Vorlagefrage zur Auslegung von Art. 82 DSGVO hat der Generalanwalt Stellung bezogen.

II. Sachverhalt

Der Fall, dem die Vorlagefragen zugrunde lagen, betraf einen Rechtsstreit zwischen einer österreichischen Privatperson und der österreichischen Post AG. Die Post AG hat mit Hilfe eines Algorithmus und sozialdemografischer Merkmale versucht, die Parteipräferenz von Personen zu ermitteln. Der Kläger hatte in diese Datenverarbeitung nicht eingewilligt und war verärgert über seine angebliche Affinität zu einer Partei. Er klagte gegen die Datenverarbeitung und verlangte den Ersatz eines immateriellen Schadens in Höhe von 1.000 Euro. Diese Schadensersatzklage wurde vom Landgericht Wien und dem Oberlandesgericht Wien aufgrund einer fehlenden Erheblichkeit der Beeinträchtigung abgewiesen. Letztinstanzlich hatte der Oberste Gerichtshof Wien über den Fall zu entscheiden. Dieser legte dem EuGH mehrere Fragen zur Auslegung von Art. 82 DSGVO vor. Diese fragten danach, ob ein Schaden nachgewiesen werden muss oder die Datenschutzverletzung bereits für einen Schadensersatzanspruch genügt und ob ein ersetzbarer immaterieller Schaden erst beim Überschreiten einer Erheblichkeitsschwelle vorliege.

III. Die Auffassung des Generalanwalts

Der Generalanwalt verfolgt in seinen Schlussanträgen ein vergleichsweise restriktives Verständnis vom immateriellen Schadensbegriff des Art. 82 DSGVO. Zunächst betont er, dass für einen Schadensersatzanspruch nicht alleine ein Verstoß gegen die Bestimmungen der DSGVO ausreicht, sondern dass stattdessen ein Schaden festgestellt werden muss, der durch den Anspruch kompensiert werden soll. Hiermit erteilt er einem extrem weiten Verständnis des Art. 82 DSGVO, das dem Schadensersatzanspruch einen primär strafenden (und nicht kompensierenden) Charakter verleiht und nicht das Entstehen eines Schadens verlangt, eine Absage. Der Generalanwalt argumentiert hierbei, dass im Unionsrecht ein Strafschadensersatz lediglich eine Ausnahme sei und weder Wortlaut der DSGVO und noch der Entstehungsgeschichte entnommen werden könne, dass Art. 82 DSGVO eine solche Funktion erfüllen soll. Stattdessen verfüge die DSGVO bereits über Maßnahmen, um Datenschutzverstöße auch unabhängig vom Vorliegen von Verschulden zu sanktionieren. So habe jede Person gemäß Art. 77 Abs. 1 DSGVO ein Recht auf Beschwerde bei einer Aufsichtsbehörde, sofern ihre personenbezogenen Daten rechtswidrig verarbeitet wurden. Die Aufsichtsbehörde können dann unterschiedliche Sanktionsmaßnahmen treffen, etwa gemäß Art. 83 DSGVO ein Bußgeld gegen den verantwortlichen Datenverarbeiter verhängen.

In gleicher Weise dürfe bei einem Datenschutzverstoß das Vorliegen eines Schadens aufgrund des entstandenen Kontrollverlusts nicht einfach vermutet werden. Der DSGVO lasse sich nicht entnehmen, dass der Kontrolle über die eigenen personenbezogenen Daten ein Wert für sich zukomme. Hierbei betont der Generalanwalt auch, dass der Schutz personenbezogener Daten nicht das ausschließliche Ziel der DSGVO sei, sondern dass auch der freie Datenverkehr gefördert werden solle.
Anschließend befasste sich der Generalanwalt mit den Voraussetzungen, die an einen immateriellen Schaden zu stellen seien. Hierbei beschäftigt er sich vor allem mit der Frage, ob es eine Erheblichkeitsschwelle für die Nachteile der betroffenen Person gebe, unter der kein Schadensersatz zu leisten sei. Diese Frage dreht sich um die Problematik, ob bereits jedes ungute Gefühl bzw. jedes Ärgernis einen ersatzfähigen Schaden darstellt. Der Generalanwalt bejaht diese Frage und möchte nicht jeden entstandenen Nachteil als ersatzfähigen immateriellen Schaden verstehen. Dies begründet er zum einen wiederum damit, dass die DSGVO nicht ausschließlich dem Schutz personenbezogener Daten diene, sondern auch den Datenverkehr fördern möchte. Zum anderen sei es auch den nationalen Rechtsordnungen immanent, dass zwischen ersatzfähigen Schäden und bloßen (nicht ersatzfähigen) Nachteilen unterschieden werde. Da zudem jeder Verstoß gegen die DSGVO negative Emotionen hervorrufe,

4 Etwa BAG, BeckRS 2021, 29622; OGH Österreich, ZD 2021, 631; LG Saarbrücken, ZD 2022, 162.

würde Art. 82 DSGVO praktisch zu einem Strafschadensersatz, beziehungsweise einem Schadensersatz ohne Schaden, wenn man jegliche negative Emotionen als Schaden anerkenne. Eine solche Funktion des Art. 82 DSGVO hatte der Generalanwalt – wie beschrieben – zuvor abgelehnt.

Der Generalanwalt betont, dass ihm bewusst sei, dass eine Unterscheidung zwischen ersatzfähigen Schäden und bloßen Nachteilen kompliziert sei, diese obliege den nationalen Gerichten.

IV. Relevanz für Hochschulen

Die Problematik datenschutzrechtlicher Schadensersatzansprüche weist eine hohe Relevanz für Hochschulen und auch andere wissenschaftliche Einrichtungen auf. Bei einem sehr weiten Verständnis des Begriffs immaterieller Schäden entsteht ein hohes Haftungsrisiko für Datenverarbeiter bei einem Datenschutzverstoß. Die Tatsache, dass Hochschulen häufig Daten von einer Vielzahl von Personen verarbeiten, verstärkt dieses Haftungsrisiko zudem, da bei einem Datenschutzverstoß dann auch eine Vielzahl von Klägern in Betracht käme. Aus der Sicht von Datenverarbeitern ist daher ein enges Verständnis immaterieller Schäden wünschenswert. Die letztverbindliche Entscheidung hierüber obliegt dem EuGH. Die Schlussanträge des Generalanwaltes haben keinen bindenden Charakter. Dennoch sollten sie beachtet werden, da die Vergangenheit gezeigt hat, dass sich der EuGH in den meisten Fällen der Auffassung des Generalanwalts angeschlossen hat. Daher erhöhen die Schlussanträge des Generalanwaltes deutlich die Wahrscheinlichkeit, dass auch der EuGH immaterielle Schäden nicht sehr weit fassen wird.

Karlsruhe zeigt Kante

Das Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns ist teilweise verfassungswidrigt

von Justin Rennert

Im Jahr 2020 hatte das Land Mecklenburg-Vorpommern sein Polzeigesetz reformiert. Nun hat das Bundesverfassungsgericht (BVerfG) Teile des neuen Gesetzes für verfassungswidrig erklärt. Dabei handelt es sich insbesondere um die Regeln zur Online-Durchsuchung und Telekommunikationsüberwachung.

I. Hintergrund

Mit dem reformierten Gesetz hatte das Land Mecklenburg-Vorpommern die Befugnisse der Sicherheitsbehörden des Landes deutlich ausgeweitet. Schon während des Gesetzgebungsverfahrens hatte es Kritik daran gegeben, unter anderem vonseiten einiger Experten in den Sitzungen des Innenausschusses und des Landesdatenschutzbeauftragten. Kritisiert wurden unter anderem die Vorschriften zur Online-Durchsuchung (auch großer Staatstrojaner genannt) und Telekommunikationsüberwachung. Trotz der Kritik hatte der Landtag das neue Sicherheits- und Ordnungsgesetz (SOG MV) im April 2020 verabschiedet. Dagegen hatten fünf Privatpersonen im Juni 2021 Verfassungsbeschwerde gegen zahlreiche Vorschriften des neuen Gesetzes eingereicht, darunter eine Rechtsanwältin, eine Klima- und Umweltaktivistin sowie ein Sozialarbeiter mit Kontakten in die Fußball-Fan-Szene. Unterstützt wurden sie dabei von der Gesellschaft für Freiheitsrechte e.V (GFF). Mit Beschluss vom 9. Dezember 2022[1] hat das Bundesverfassungsgericht über die Verfassungsbeschwerde entschieden und die angegriffenen Vorschriften für verfassungswidrig erklärt. Der Landesgesetzgeber hat nun bis zum Ende dieses Jahres Zeit, für neue, verfassungskonforme Regeln zu sorgen. Die GFF hofft, dass die Entscheidung Signalwirkung auch für andere Bundesländer entfaltet. Denn auch zahlreiche andere Bundesländer haben in den letzten Jahren die Befugnisse ihrer Sicherheitsbehörden ausgeweitet.

II. Die Entscheidung im Einzelnen

Im Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern sind die Kompetenzen der Ordnungsbehörden und der Polizei des Landes Mecklenburg-Vorpommern festgelegt. Die Behörden dürfen nur diejenigen Überwachungsmaßnahmen durchführen, die auch im Gesetz niedergeschrieben sind. Die Verfassungsbeschwerde richtete sich gleich gegen eine Vielzahl von Überwachungsmaßnahmen. Für verfassungswidrig erklärte das Bundesverfassungsgericht die Vorschriften zur längerfristigen Observation von Verdächtigen, zur Wohnraumüberwachung, zur Online-Durchsuchung, zur Telekommunikationsüberwachung und zur Rasterfahndung. Die Entscheidung bedeutet nicht, dass diese Maßnahmen generell unzulässig sind. Das mecklenburgische Gesetz sehe allerdings durchweg zu niedrige Voraussetzung für die Durchführung derartiger Maßnahmen vor, so das BVerfG.[2] So waren Online-Durchsuchung und Telekommunikationsüberwachung nach dem reformierten Gesetz schon dann möglich, wenn Anhaltspunkte für Vorbereitungshandlungen gewisser Straftaten vorlagen. Eine konkrete Gefahr für Rechtsgüter war nicht erforderlich. Die Online-Durchsuchung ermöglicht die Infiltration eines IT-Systems mittels Ausspähsoftware und wird deswegen auch großer Staatstrojaner genannt. Behörden können dann auf sämtliche auf dem System gespeicherte Daten zugreifen. Die Telekommunikationsüberwachung ermöglicht die Überwachung und Aufzeichnung von Kommunikationsinhalten

1 BVerfG, Beschluss v. 09. Dezember 2022 - 1 BvR 1345/21.

2 Zu den verfassungsrechtlichen Grundlagen: Gielen, „Die Sicherheit unserer Daten“ in DFN-Infobrief Recht 07/2019.

durch den Einsatz technischer Mittel.[3] Beide Maßnahmen gehen mit erheblichen Grundrechtseingriffen einher; betroffen sind unter anderem das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sowie das Fernmeldegeheimnis. Wenn ein Gesetz derart niedrige Voraussetzungen für derart intensive Grundrechtseingriffe vorsieht, so widerspräche das dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit, so das BVerfG.

Gleiches gelte für die Vorschriften zur Wohnraumüberwachung. Diese ermöglichen den Behörden, durch den verdeckten Einsatz technischer Mittel in oder aus der Wohnung einer Person deren nichtöffentlich gesprochenes Wort abzuhören oder Lichtbilder und Bildaufzeichnungen herzustellen. Nach dem BVerfG sei die Wohnraumüberwachung nur zulässig bei einer dringenden Gefahr für die öffentliche Sicherheit.

III. Fazit und Bedeutung für Forschung und Hochschulen

Das BVerfG hat einige der angegriffenen Vorschriften für nichtig erklärt, andere wiederum „nur" für verfassungswidrig. In beiden Fällen muss der Landesgesetzgeber nun Nachfolgevorschriften schaffen. Die nichtigen Vorschriften sind mit sofortiger Wirkung unanwendbar, die verfassungswidrigen Vorschriften bleiben mit Einschränkungen bis zum 31. Dezember 2023 anwendbar (zeitlich beschränkte Fortgeltung). Das BVerfG kann die zeitlich beschränkte Fortgeltung anordnen, wenn ansonsten keine Rechtsgrundlage mehr für den Schutz überragender Güter des Gemeinwohls bestünde. Es ist dann aber nicht so, dass die Behörden im Übergangszeitraum mit der Absolution des BVerfG verfassungswidriges Recht anwenden dürften. Die durch das BVerfG angeordneten Einschränkungen sorgen jedoch schon im Übergangszeitraum für Verfassungskonformität.

Der Landesdatenschutzbeauftragte des Landes Mecklenburg-Vorpommern reagierte in einer Pressemitteilung: Er hoffe, dass die Hinweise seiner Behörde bei der Neufassung des Gesetzes berücksichtigt würden.[4] Die GFF sah in dem Urteil einen „Erfolg für die Freiheitsrechte" und betonte, dass das Urteil über Mecklenburg-Vorpommern hinaus Bedeutung haben würde.[5] Tatsächlich hat das BVerfG mit der Entscheidung erkennen lassen: Online-Durchsuchung und Telekommunikationsüberwachung sollen nur dann möglich sein, wenn mindestens eine konkretisierte Gefahr für Rechtsgüter gegeben ist. Für die Forschung ist die Entscheidung ein Signal dergestalt, dass das BVerfG das Recht auf informationelle Selbstbestimmung und das IT-Grundrecht gegenüber verschärften Sicherheits- und Ordnungsgesetzen stärkt. In diese Richtung deutet auch das jüngste Urteil des BVerfG zu den Sicherheitsgesetzen in Hessen und Hamburg:[6] Das Gericht hatte diese Gesetze ebenfalls für teilweise verfassungswidrig erklärt. Diese sähen für die automatisierte Analyse personenbezogener Daten zu geringe Voraussetzungen vor. Das Gericht begründet seine Entscheidung ebenso wie die Entscheidung zum SOG Mecklenburg-Vorpommern demnach mit Verhältnismäßigkeitserwägungen.

---

3 Detailliert hierzu: Rennert, „Handy weg? EncroChat" in DFN-Infobrief Recht 03/2022.

4 Pressemitteilung des Landesdatenschutzbeauftragten, abrufbar unter: https://www.datenschutz-mv.de/presse/?id=188008&processor=processor.sa.pressemitteilung – zuletzt abgerufen am 7. Februar 2023.

5 Pressemitteilung der Gesellschaft für Freiheitsrechte e.V., abrufbar unter: https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-erfolg-sog-mv - zuletzt abgerufen am 7. Februar 2023.

6 BVerfG, Urteil v. 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20.

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