Kommunikation & Recht

K&R
5 | Mai 2025
28. Jahrgang
Seiten 289 -360

Verderben (zu) viele Köche den Brei?
Dr. Kristina Schreiber

289 Schutz vor Stilnachahmungen durch generative KI
Dr. Felix Rützel

292 Der Anspruch auf Erläuterung automatisierter Entscheidungen unter der DSGVO
David Pfahler

295 Gastzugang im Onlinehandel – muss das sein?
Dr. Moritz Indenhuck

298 Kontrollverlust und datenschutzrechtlicher Schadensersatzanspruch bei unerwünschter E-Mail-Werbung
Dr. Sascha Vander

302 Update: Besteuerung der digitalen Wirtschaft 2024/2025 – Teil 2
Prof. Dr. Jens M. Schmittmann und Prof. Dr. Julia Sinnig

310 **EuGH:** Unternehmensbegriff bei DSGVO-Bußgeldern

316 **BGH:** Immaterieller Schaden durch unberechtigten Schufa-Eintrag

318 **BGH:** App-Zentrum III: Unzureichende datenschutzrechtliche Information zugleich Verstoß gegen Lauterkeitsrecht

324 **BGH:** Arzneimittelbestelldaten II: Verarbeitung der Bestelldaten ohne Einwilligung als Verstoß gegen Marktverhaltensregelung

329 **BGH:** Arzneimittelbestelldaten III: Schadensersatzanspruch bei unklarer Rechtslage

330 **BGH:** Mindestbeschwer bei unwirksamer Klausel zur Abo-Preisanpassung

338 **OLG Köln:** Gesellschafter haftet trotz Counter-Notification nicht für YouTube-Videos

345 **OLG Frankfurt a. M.:** Unzulässige Berichterstattung über Promi-Beziehung

351 **LG Köln:** Verlagshaftung für Inhalt eines Google-Snippets möglich mit Kommentar von **Dr. Karolin Nelles**

355 **BVerwG:** Auch digitale Presse unterfällt dem Schutz der Pressefreiheit

dfv Mediengruppe
Frankfurt am Main

möglichkeit eingeräumt wird. Dies lasse erkennen, dass der (Unions)Gesetzgeber auch die vorgelagerte Auswertung der Bestellhistorie ohne Einwilligung ermöglichen wollte.

IV. Fazit

Mit seiner Entscheidung liefert das OLG Hamburg wichtige Konkretisierungen für die datenschutzkonforme Ausgestaltung von Vertriebsplattformen im Onlinehandel. Das Gericht stellt klar, dass der Grundsatz der Datenminimierung keinen pauschalen Zwang zu Gastzugängen begründet. Vielmehr ist im Einzelfall zu prüfen, ob die mit einer dauerhaften Registrierung verbundene Datenverarbeitung für den konkreten Geschäftszweck erforderlich und verhältnismäßig ist.

Insbesondere die vom OLG vorgenommene Einordnung des DSK-Beschlusses dürfte E-Commerce-Plattformen praktikable Handlungsspielräume aufzeigen. Indem das Gericht die Ausgestaltung des Kundenkontos im vorliegenden Fall aufgrund „besonderer Umstände" für zulässig hält, relativiert es das im DSK-Beschluss angelegte Regel-Ausnahme-Verhältnis erheblich. Mit ähnlichen Erwägungen dürfte sich auch für eine Vielzahl weiterer Anbieter ein vergleichbares Registrierungserfordernis rechtfertigen lassen.

Für die Praxis bedeutsam ist zudem die differenzierte Betrachtung einzelner Datenkategorien, bei der das OLG insbesondere die Erhebung von Telefonnummer und Geburtsdatum für bestimmte Zwecke wie Betrugsprävention legitimiert.

Auch hinsichtlich der werblichen Nutzung von Bestellhistorien nimmt das Gericht eine praxisorientierte Position ein. Es betont, dass keine generelle Einwilligungsbedürftigkeit besteht, sondern eine Direktwerbung gegenüber Bestandskunden auf berechtigte Interessen gestützt werden kann, sofern die entsprechenden gesetzlichen Rahmenbedingungen eingehalten werden.

Insgesamt trägt die Entscheidung zur Rechtssicherheit im E-Commerce bei, indem sie einen ausgewogenen Mittelweg zwischen überzogenen Datenschutzanforderungen und ausufernder Datenakkumulation durch Anbieter aufzeigt. Der Grundsatz der Datenminimierung wird nicht als starres Prinzip minimaler Datenerfassung verstanden, sondern als Gebot verhältnismäßiger, zweckgebundener und transparent kommunizierter Datenverarbeitung. Damit setzt das OLG Hamburg einen pragmatischen Maßstab, der sowohl dem Schutzzweck der DSGVO als auch den praktischen Erfordernissen des modernen Onlinehandels Rechnung trägt.

Dr. Moritz Indenhuck
ist Rechtsanwalt mit den Schwerpunkten Datenschutzrecht, Künstliche Intelligenz und IT-rechtliche Vertragsgestaltung. Er berät Anbieter von Online-Services, Technologieunternehmen sowie regulierte Unternehmen der Finanzwirtschaft. Als ausgebildeter Softwareentwickler bringt er sein Know-how in interdisziplinären Projekten ein.

RA Dr. Sascha Vander, LL.M.*

Kontrollverlust und datenschutzrechtlicher Schadensersatzanspruch bei unerwünschter E-Mail-Werbung

Zugleich Kommentar zu BGH, Urteil vom 28. 1. 2025 – VI ZR 109/23, K&R 2025, 261 ff. (Heft 4)

Kurz und Knapp

Der BGH hat datenschutzrechtlichen Schadensersatzansprüchen im Kontext unerwünschter E-Mail-Werbung Grenzen gesetzt und seine Rechtsprechung in Sachen „Kontrollverlust" präzisiert. Ein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO sei nicht hinreichend dargelegt, wenn ein auf einem gerügten Verstoß beruhender Kontrollverlust über personenbezogene Daten nicht vorliegt und auch die geäußerte Befürchtung eines Kontrollverlusts nicht substantiiert dargelegt wird.

I. Hintergrund

1. Kontrollverlust im Fokus

Spätestens seit den viel beachteten EuGH-Entscheidungen in Sachen datenschutzrechtlicher Kontrollverlust[1] und Schadensersatz[2] ist der datenschutzrechtliche Schadensersatzanspruch Betroffener noch stärker in den Fokus gerückt.

2. Scraping-Verfahren in Deutschland

Die Flut der in Deutschland anhängigen Verfahren gegen Facebook in Sachen Scraping und zum Schadensersatz verpflichtender Kontrollverlust spricht insoweit eine klare Sprache und hatte den BGH im November 2024 dazu veranlasst, eines der betroffenen Verfahren auf Grundlage einer unlängst in Kraft getretenen Neuregelung in der ZPO (vgl. § 552b ZPO

* Mehr über den Autor erfahren Sie am Ende des Beitrags.

1 Zur normativen Verankerung des „Kontrollverlusts" siehe Erwägungsgrund Nr. 85 DSGVO.

2 EuGH, 4. 10. 2024 – C-200/23, K&R 2025, 29 ff. = ZD 2025, 87; EuGH, 20. 6. 2024 – C-590/22, K&R 2024, 503; EuGH, 11. 4. 2024 – C-741/21, K&R 2024, 342 ff., Rn. 42; EuGH, 25. 1. 2024 – C-687/21, K&R 2024, 192 ff., Rn. 66; EuGH, 14. 12. 2023 – C-456/22, K&R 2024, 112 ff., Rn. 18 - 23.

n. F.) zu einem sog. Leitentscheidungsverfahren zu erklären.[3] Der BGH legte im Kontext streitiger Schadensersatzansprüche den Fokus auf die Frage, ob ein bloßer Verlust über die Kontrolle von Daten einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO darstellen kann und wie ein etwaig gebotener Ersatz für einen solchen Schaden zu bemessen wäre. Zudem rückte der BGH die Substantiierungslast ins Zentrum und warf die zusätzliche Frage auf, welche Anforderungen an die Substantiierung einer auf Art. 82 DSGVO gestützten Schadensersatzklage zu stellen sind.

Die Entscheidung des BGH wurde mit Spannung erwartet und erfolgte bereits 14 Tage nach der Bestimmung des betroffenen Verfahrens zum Leitverfahren.[4] Mit Blick auf die mangelnde Rücknahme der Revision und eine ebenfalls ausgebliebene anderweitige Erledigung erfolgte zwar keine Leitentscheidung gemäß § 565 ZPO, sondern ein „normales" Urteil mit nicht minder großer Sprengkraft.

a) Niederschwellige Anforderung an immaterielle Schäden

Nach der für die Auslegung des Art. 82 Abs. 1 DSGVO maßgeblichen Rechtsprechung des EuGH könne auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die DSGVO einen immateriellen Schaden im Sinne der Norm darstellen. Die Anforderungen für den Nachweis eines vermeintlichen Schadens setzte der BGH vergleichsweise niedrig an. Weder müsse insoweit eine konkrete missbräuchliche Verwendung der Daten zum Nachteil des Betroffenen erfolgt sein noch bedürfe es sonstiger zusätzlicher spürbarer negativer Folgen.

Die Entscheidung eröffnete damit jedenfalls einen Argumentationsspielraum dahingehend, dass bereits der Nachweis eines Anspruchstellers, von einem Scraping-Vorfall betroffen gewesen zu sein, Schadensersatzansprüche begründen konnte. Da der BGH nicht den Nachweis einer konkreten missbräuchlichen Verwendung der Daten zum Nachteil des Betroffenen oder sonstige – neben dem reinen Kontrollverlust – zusätzliche spürbare negative Folgen verlangte, machte sich im unternehmerischen Bereich die Sorge breit, dass sich Schadensersatzansprüche namentlich bei Datenschutzvorfällen zu einem Selbstläufer entwickeln könnten.

b) Wirtschaftliche Folgen

Auch wenn der BGH für den Fall eines reinen Kontrollverlustes – betroffen waren allerdings keine besonders sensiblen Daten – die Höhe eines Schadensersatzanspruchs tendenziell zurückhaltend mit rund EUR 100,00 bewertete, dürfte dies betroffenen Unternehmen bei der in solchen Konstellationen nicht selten erheblichen Anzahl Betroffener nur bedingt helfen. So waren von dem Facebook-Vorfall allein in Deutschland rund sechs Millionen Personen betroffen.[5] Auch wenn nur ein Teil der Betroffenen Ersatzansprüche in Höhe von EUR 100,00 verfolgen würde, käme eine beträchtliche Gesamtforderung zustande. Auch der unternehmensinterne Aufwand, der mit der Verfolgung von Ansprüchen durch eine Vielzahl Betroffener einhergeht, ist nicht zu unterschätzen und einzupreisen. Gerade bei systembedingten Datenschutzverstößen oder einem Datenschutzvorfall kann die Zahl potentiell Betroffener in die Höhe schnellen und mit Blick auf die Kumulation zahlreicher Einzelansprüche ein erhebliches wirtschaftliches Risiko begründen.[6]

c) Einfallstor für Massenverfahren

Die Entscheidung des BGH wirkte wie Wasser auf die Mühlen bereits aktiver und anderweitig in den Startlöchern stehender Betreiber bzw. Anbieter von Massenverfahren.[7] Eine erst wenige Wochen vor der BGH-Entscheidung ergangene Entscheidung des Bundessozialgerichts, welche mit Blick auf eine tendenziell strengere Bewertung der Substantiierungslast etwaige datenschutzrechtlichen Ersatzansprüchen in Fällen eines vermeintlichen „Kontrollverlusts" Grenzen aufzeigte,[8] drohte in den Hintergrund zu treten. Ungeachtet dessen ist die Entscheidung des Bundessozialgerichts nach wie vor interessant, da das Gericht im betreffenden Fall eine vergleichsweise klare Grenzziehung zwischen einem tatsächlichen Kontrollverlust und einem „hypothetischen" Kontrollverlust[9] vorgenommen hat – ein Aspekt, auf den im Kontext der in diesem Beitrag im Zentrum stehenden Erwägungen des BGH in Sachen Kontrollverlust und datenschutzrechtlicher Schadensersatzanspruch bei unerwünschter E-Mail-Werbung zurückzukommen ist.

3. Kontrollverlust und E-Mail-Werbung

Dem BGH bot sich nunmehr erneut Gelegenheit, sich zu den Anforderungen an einen datenschutzrechtlichen Schadensersatzanspruch im Kontext eines vermeintlichen Kontrollverlusts zu positionieren.[10]

Die Entscheidung ist in der Praxis durchaus mit Spannung erwartet worden, da das ohnehin höchst streitanfällige Thema der unerwünschten E-Mail-Werbung mit datenschutzrechtlichen Schadensersatzansprüchen infolge eines vermeintlichen „Kontrollverlusts" kombiniert wurde. Insoweit ist insgesamt das Phänomen zu beobachten, dass Fälle unerwünschter E-Mail-Werbung zunehmend weniger im lauterkeitsrechtlichen Bereich eine Rolle spielen und der Schwerpunkt sich vielmehr in Richtung Persönlichkeitsrecht und Schadensersatzforderungen verschoben hat. Eine im Kontext unerwünschter E-Mail-Werbung großzügige Handhabung datenschutzrechtlicher Schadensersatzansprüche wegen eines ggf. nicht feststehenden, sondern nur – was nach der EuGH- und BGH-Rechtsprechung ausreichen kann – „befürchteten" Kontrollverlusts könnte einmal mehr die Grundlage für ein auf Massenverfahren angelegtes Geschäftsmodell bilden. Dass in solchen Fällen vielfach nicht die Abwehr etwaiger Persönlichkeitsrechtsverletzungen im Fokus steht, sondern schlicht die Generierung von Einnahmen, soll an dieser Stelle nicht weiter vertieft und bewertet werden.

II. Sachverhalt

Die Parteien stritten um immateriellen Schadensersatz wegen einer behaupteten Verletzung der DSGVO.

Der Kläger kaufte vom Beklagten Aufkleber. Mit einer nachfolgenden E-Mail meldete sich der Beklagte beim Kläger und warb damit, weiterhin für ihn da zu sein. Der Kläger über-

3 BGH, 31. 10. 2024 – VI ZR 10/24, K&R 2025, 317 f. (in diesem Heft).
4 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35.
5 Zur Dimension des Themenkomplexes Facebook-Scraping vgl. *Toussaint*, FD-ZVR 2024, 824428.
6 *Solmecke*, DSB 2024, 314, 316 und *Mantz*, GRUR, 2024, 1878, 1881 weisen für die Anspruchsteller zutreffend auf die für Kleinschäden relevanten Möglichkeiten einer Abtretung an Prozesskostenfinanzierer oder eine Bündelung über § 15 Abs. 1 VDuG hin.
7 *Spittka*, DSB 2024, 311, 313 wies auf die Gefahr einer „Kommerzialisierung von Datenlecks und Datenschutzvorfällen" hin.
8 BSG, 24. 9. 2024 – B 7 AS 15/23, ZD 2025 m. Anm. *Viehweger*.
9 BSG, 24. 9. 2024 – B 7 AS 15/23, Rn. 31, ZD 2025, 110.
10 BGH, 28. 1. 2025 – IV ZR 109/23, K&R 2025, 261.

sandte dem Beklagten noch am selben Tag eine E-Mail, mit der er der „Verarbeitung oder Nutzung“ seiner Daten „für Zwecke der Werbung oder der Markt- oder Meinungsforschung auf jeglichem Kommunikationsweg“ widersprach. Er verlangte neben der Abgabe einer strafbewehrten Unterlassungserklärung auch „Schmerzensgeld gem. Art. 82 DSGVO“ in Höhe von EUR 500,00.

Mit seiner Klage hat der Kläger beantragt, dem Beklagten zu untersagen, den Kläger per E-Mail zu Werbezwecken ohne seine Einwilligung zu kontaktieren. Außerdem hat er beantragt, den Beklagten zur Zahlung eines angemessenen „Schmerzensgeldes“ in Höhe von mindestens EUR 500,00 nebst Zinsen zu verurteilen. Der Beklagte hat den Unterlassungsantrag anerkannt. Das AG hat den Beklagten gemäß seinem Teilanerkenntnis verurteilt und im Übrigen die Klage abgewiesen sowie die Berufung zugelassen. Das LG hat die Berufung des Klägers zurückgewiesen. Mit der vom Berufungsgericht zugelassenen Revision verfolgt der Kläger seinen Zahlungsantrag weiter.

III. Wesentliche Erwägungen

Die zulässige Revision hatte in der Sache keinen Erfolg. Das Berufungsgericht habe – so der BGH – im Ergebnis zu Recht einen Anspruch des Klägers auf Ersatz von immateriellem Schaden nach Art. 82 Abs. 1 DSGVO verneint.

1. Keine Bagatellgrenze

Das Berufungsgericht sei zwar im Ausgangspunkt unzutreffend davon ausgegangen, dass dem Kläger schon deshalb kein Anspruch auf immateriellen Schadensersatz zustehe, da eine „Bagatellgrenze“ nicht überschritten sei. Ein solcher Ansatz stehe nicht in Einklang mit der Rechtsprechung des EuGH, wonach Art. 82 DSGVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat.[11]

2. Darlegung und Substantiierung eines Schadens

Das Berufungsgericht habe einen Anspruch des Klägers aber zu Recht verneint, weil der Kläger einen immateriellen Schaden bereits nicht hinreichend dargelegt habe.

a) Eigenständige Anspruchsvoraussetzung

Die Ablehnung einer Erheblichkeitsschwelle durch den EuGH bedeute nicht, dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen. Der bloße Verstoß gegen die Bestimmungen der DSGVO reiche nach der Rechtsprechung des Gerichtshofs nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr sei darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens durch diesen Verstoß erforderlich.[12]

b) Tatsächlicher Kontrollverlust oder objektivierbare Befürchtung

Aus dem Vortrag des Klägers ergebe sich nicht, dass dem Kläger durch die Verwendung seiner E-Mail-Adresse ohne Einwilligung zum Zweck der Zusendung einer Werbe-E-Mail ein immaterieller Schaden entstanden wäre. Es liege weder ein auf dem gerügten Verstoß beruhender Kontrollverlust des Klägers über seine personenbezogenen Daten vor, noch sei die vom Kläger geäußerte Befürchtung eines Kontrollverlusts substantiiert dargelegt.

Der EuGH habe in seiner jüngeren Rechtsprechung klargestellt, dass schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen könne, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordere. Gleichwohl müsse die betroffene Person den Nachweis erbringen, dass sie einen solchen – d. h. in einem bloßen Kontrollverlust als solchem bestehenden – Schaden erlitten habe. Stehe der Kontrollverlust fest, stelle dieser selbst den immateriellen Schaden dar und es bedürfe keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person.

Dem klägerischen Vortrag sei nicht zu entnehmen gewesen, dass der Kläger aufgrund der Verwendung seiner E-Mail-Adresse zur Übersendung der streitgegenständlichen E-Mail einen Kontrollverlust über seine personenbezogenen Daten erlitten hätte. Ein Kontrollverlust könne allenfalls dann vorliegen, wenn der Beklagte die Daten des Klägers mit der Übersendung der Werbe-E-Mail zugleich Dritten zugänglich gemacht hätte.[13] Das sei aber nicht der Fall gewesen.

Wenn ein Kontrollverlust nicht nachgewiesen werden könne, reiche die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, aus, um einen Schadensersatzanspruch zu begründen. Die Befürchtung samt negativer Folgen müsse dabei ordnungsgemäß nachgewiesen sein; demgegenüber genüge die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten.[14]

Den Vortrag des Klägers, wonach die Befürchtung bestehe, der Beklagte werde die E-Mail-Adresse des Klägers auch Dritten zugänglich machen, da er die E-Mail-Adresse bereits unbefugt gegenüber dem Kläger verwendet habe, ließ der BGH nicht genügen. Der Kläger lege insoweit nur die – im Übrigen aus sich heraus nicht ohne Weiteres nachvollziehbare – Befürchtung weiterer Verstöße gegen die DSGVO durch den Beklagten dar.[15]

IV. Einordnung und Auswirkungen

1. Praktische Relevanz

Die praktische Relevanz der Entscheidung kann gar nicht unterschätzt werden. Wäre der BGH der Argumentation des Klägers gefolgt und hätte allein den Versand einer unerwünschten Werbe-E-Mail als solchen und eine vermeintlich daraus resultierende Befürchtung eines Kontrollverlusts bzw. einer etwaigen sonstigen rechtswidrigen Verwendung der E-Mail-Adresse zur Darlegung eines relevanten Kontrollverlustschadens genügen lassen, wäre Schadensersatzforderungen bei unerwünschter E-Mail-Werbung Tür und Tor geöffnet worden.

11 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 9, K&R 2025, 261, 262.
12 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 12, K&R 2025, 261, 262.
13 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 18, K&R 2025, 261, 262.
14 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 19, K&R 2025, 261, 262.
15 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 20, K&R 2025, 261, 262.

Die Begründung der Befürchtung eines vermeintlichen Kontrollverlusts war nämlich höchst allgemein gehalten und knüpfte im Ergebnis eher an die Frage nach einer Wiederholungsgefahr als an einen Kontrollverlust im konkreten datenschutzrechtlichen Kontext an. So stellte die Revision darauf ab, dass durch Zusendungen der in Rede stehenden Art das „ungute Gefühl" erweckt werde, dass personenbezogene Daten Unbefugten bekannt gemacht worden seien, gerade weil die Daten unbefugt verwendet worden seien. Der Kläger habe sich mit der Abwehr der von ihm unerwünschten Werbung und der Herkunft der Daten auseinandersetzen müssen, was zu einem „durchaus belastenden Eindruck des Kontrollverlusts" geführt habe. Außerdem habe der Beklagte nach dem Verstoß zunächst einmal nicht reagiert, was eine erneute „Missachtung des Klägers" zum Ausdruck bringe.

2. Tatsächlicher Kontrollverlust

Dass der BGH einen tatsächlichen Kontrollverlust nicht nachvollziehen konnte, dürfte kaum verwundern. Allein aus der unbefugten Verwendung von Daten des Klägers zur Versendung einer unerwünschten werblichen E-Mail lässt sich nun einmal besten Willens nicht ableiten, dass betroffene Daten des Betroffenen dann auch von Dritten entsprechend verwendet werden. Der Kläger unterstellte im Ergebnis schlicht, dass ein Verantwortlicher, der unerwünschte werbliche E-Mails versendet, seine Daten auch Dritten zum Zwecke des Versandes werblicher E-Mails zur Verfügung stellt. Sofern – wie im vorliegenden Fall – keinerlei objektive Anhaltspunkte für eine solche Verfahrensweise vorliegen, erschöpft sich betreffender Vortrag in einer schlichten Unterstellung ohne Substanz.

Ungeachtet dessen würde ein solcher Ansatz den relevanten Schadenskontext überdehnen. Dieser ist auf den Schaden durch die vermeintlich kausale Handlung beschränkt. Wenn die angegriffene Schadenshandlung hingegen in dem Versand einer unerwünschten werblichen E-Mail besteht, kann sich ein relevanter Schaden schwerlich aus einer davon losgelösten, weiteren und eben nur befürchteten Handlung des Verantwortlichen ergeben – hier eine befürchtete Weitergabe von Daten vom Verantwortlichen an einen Dritten für den Versand werblicher Nachrichten. Nimmt man dies in den Blick, erscheint auch die Feststellung des BGH konsequent, wonach ein Kontrollverlust – infolge des streitgegenständlichen Versandes der unerwünschten werblichen E-Mail – allenfalls dann vorliegen könnte, wenn der Beklagte die Daten des Klägers mit der Übersendung der Werbe-E-Mail zugleich Dritten zugänglich gemacht hätte.[16]

3. Befürchteter Kontrollverlust

Wichtiger und in der Sache entscheidungserheblich war allerdings die Feststellung des BGH, dass ungeachtet des in tatsächlicher Hinsicht nicht nachgewiesenen Kontrollverlusts auch die Darlegung einer schadensbegründenden Befürchtung unzureichend war. Für die Praxis von besonderer Relevanz erscheint insoweit, dass die vom Kläger angeführten Bemühungen zur Abwehr der unerwünschten Werbung nach Ansicht des BGH schon für sich nicht zur Begründung des behaupteten Eindrucks eines Kontrollverlusts ausreichten. Mit anderen Worten: Der möglicherweise mit dem Erhalt unerwünschter E-Mail-Werbung verbundene Ärger und Abwicklungsaufwand als solcher – so wird teilweise immer noch etwa der vermeintlich mit dem Aussortieren werblicher E-Mails entstehende Zeitaufwand als relevanter Schadensfaktor angeführt – ist jedenfalls unter dem Gesichtspunkt des datenschutzrechtlichen Schadensersatzanspruchs mit Blick auf einen vermeintlichen Kontrollverlust nicht durchsetzbar.[17]

4. Objektivierbarkeit vermeintlicher Befürchtungen

Dass ein anderweitiges Ergebnis mit den im Übrigen an eine Verletzung des allgemeinen Persönlichkeitsrechts gestellten Anforderungen zur Begründung immateriellen Schadensersatzes eine ganz erhebliche Schieflage gebildet hätte, kann zwar nicht als Argument gegen die für datenschutzrechtliche Schadensersatzansprüche nun einmal nicht zu bewertende Frage einer Schadenserheblichkeit ins Feld geführt werden. Wenn aber schon die Befürchtung eines Datenkontrollverlusts zur Begründung von datenschutzrechtlichen Schadensersatzansprüchen genügen soll, sind jedenfalls die Anforderungen an die substantiierte Darlegung einer entsprechenden Befürchtung samt ihren negativen Folgen nicht zu gering anzusetzen.

Wenn objektiv kein Kontrollverlust festgestellt, gleichwohl die Befürchtung eines solchen als hinreichende Schadensgrundlage angenommen werden kann, muss eine solche Befürchtung zumindest objektivierbar sein und darf nicht allein von vermeintlichen, rein subjektiven Befindlichkeiten des Betroffenen abhängen.

Dass der BGH in seiner Entscheidung genau an diesem Punkt angesetzt hat, erscheint auch mit Blick auf die einschlägige Rechtsprechung des EuGH nicht nur vertretbar, sondern geradezu geboten. So hat der EuGH entschieden, dass Art. 82 Abs. 1 DSGVO dahin auszulegen ist, dass die Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen diese Verordnung an Dritte weitergegeben wurden, ohne dass nachgewiesen werden kann, dass dies tatsächlich der Fall war, ausreicht, um einen Schadensersatzanspruch zu begründen, sofern diese Befürchtung samt ihren negativen Folgen ordnungsgemäß nachgewiesen ist.[18] Auch der EuGH stellte also nicht schlicht auf den Nachweis einer vermeintlichen und möglicherweise stark subjektiv geprägten Befürchtung als solcher, sondern auch die betroffenen negativen Folgen ab – im Ergebnis eine Objektivierung der im Übrigen eher subjektiv gefärbten Voraussetzung einer „Befürchtung".

Insoweit schließt sich dann auch der Kreis zur eingangs erwähnten Entscheidung des Bundessozialgerichts,[19] welches datenschutzrechtlichen Schadensersatzansprüchen aufgrund einer nicht hinreichend substantiierten Befürchtung eines Kontrollverlusts und dessen Folgen schon im vergangenen Jahr eine Absage erteilt hatte.

Kurzum: Wenn ein datenschutzrechtlicher Schadensersatzanspruch ungeachtet eines objektiv nicht feststellbaren Kontrollverlusts allein aufgrund einer entsprechenden Befürchtung verfolgt werden soll, müssen für die vermeintliche Befürchtung und die vermeintlichen negativen Folgen objektivierbare und belastbare Darlegungen erfolgen. Dies wird in Fällen unerwünschter E-Mail-Werbung allenfalls in Ausnahmefällen relevant sein können, wobei hier im Wesentlichen eine datenschutzwidrige Weitergabe oder Offenlegung von personenbe-

16 BGH, 28. 1. 2025 – IV ZR 109/23, Rn. 18, K&R 2025, 261, 262.

17 Das AG Goslar, 22. 1. 2024 – 28 C 7/19, ZD 2024, 771 hatte in einer viel beachteten, allerdings wenig überzeugenden Begründung einen Schmerzensgeldanspruch unter dem Gesichtspunkt der Lästigkeit und des entstehenden Aufwandes unter Art. 82 Abs. 1 DSGVO angenommen und der Höhe nach mit EUR 25.00 zugesprochen. Ablehnend: AG Hamburg-Bergedorf, 7. 12. 2020 – 410 d C 197/20.

18 Siehe insbesondere EuGH, 20. 6. 2024 – C-590/22 (Antwort Vorlagefrage Nr. 3), K&R 2024, 503 mit weiteren Nachweisen der einschlägigen EuGH-Rechtsprechung.

19 BSG, 24. 9. 24 – B 7 AS 15/23, Rn. 31, ZD 2025, 110.

zogenen Daten relevant sein wird. In diesen Fällen mag es dann zwar auch mittelbar um unerwünschte E-Mail-Werbung gehen, den Kern des einen datenschutzrechtlichen Schadensersatzanspruch unter dem Gesichtspunkt eines Kontrollverlustes auslösenden Faktors wird dann aber nicht die Frage nach einer etwaig mangelnden Einwilligung im Sinne von § 7 Abs. 2 Nr. 2 UWG, sondern vielmehr ein sonstiger Datenschutzverstoß, z. B. eine unerlaubte Weitergabe, bilden.

5. Weitere Entwicklung und Tendenzen

Im Übrigen ist aktuell nach hiesigem Eindruck eine Tendenz dahingehend zu beobachten, dass namentlich die obergerichtliche Rechtsprechung in Deutschland in Sachen Kontrollverlust und Schadensersatz eine restriktivere Linie verfolgt und die Anforderungen an die Substantiierung eines Kontrollverlusts und erst recht an einen befürchteten Kontrollverlust nicht zu gering ansetzt. Hatte zunächst zum Teil mit Blick auf die BGH-Entscheidung in Sachen Facebook-Scraping die Annahme bestanden, dass sich insbesondere die Facebook-Fälle zu einer Art „Selbstläufer" entwickeln, scheint sich diese Annahme nicht zu bewahrheiten. Die Gerichte gehen zum Teil vielmehr sehr kleinteilig vor und prüfen genau, ob und inwiefern überhaupt ein Kontrollverlust in Rede steht bzw. dargelegt ist und inwiefern etwaige Befürchtungen einer objektivierbaren Darlegung genügen.[20] Kläger, die sich auf einen schlichten Verweis darauf beschränken, von einem „Vorfall betroffen" zu sein, sind jedenfalls schlecht beraten.

Interessant erscheint eine vom OLG Dresden getroffene Feststellung einer jedenfalls im Ausgangspunkt denkbaren Substantiierung eines möglichen Kontrollverlusts. So sei das Angebot der Webseite www.haveibeenpwnd.com hinreichend verlässlich, um jedenfalls die individuelle Betroffenheit von Sicherheitsvorfällen darzulegen und damit die sekundäre Darlegungslast des Betreibers auszulösen.[21] Auf www.haveibeenpwnd.com lässt sich feststellen, ob eine bestimmte E-Mail-Adresse und ggf. mit der E-Mail-Adresse verknüpfte weitere Daten einem bekannt gewordenen Datenleak bzw. einer entsprechenden Datensammlung zuzuordnen sind. Da die betreffenden Leaks regelmäßig im Darknet verfügbar gemacht werden und oftmals auch fortlaufend verfügbar sind, könnte in Bezug auf die betroffenen Daten grundsätzlich von einem Kontrollverlust auszugehen sein. Die Belastbarkeit eines solchen Nachweises wird von Teilen der Rechtsprechung allerdings mit Verweis auf eine vermeintlich mangelnde Verlässlichkeit bzw. Aussagekraft in Abrede gestellt.[22]

Aber selbst für den Fall, dass im Ausgangspunkt hinreichende Anhaltspunkte für einen Kontrollverlust vorgetragen werden, muss gleichwohl nicht zwingend ein solcher angenommen werden. Ausgehend von der Annahme, dass ein Kontrollverlust nun einmal nur eintreten kann, wenn der Betroffene bzw. Anspruchsteller die betroffenen Daten vorher „unter Kontrolle hatte", kann ein „datenfreizügiger" Umgang einer Kontrollverlust-Argumentation die Grundlage entziehen, z. B. bei einer selbst veranlassten öffentlichen Wiedergabe von Daten in sozialen Medien oder auch auf der eigenen Website.[23] Gleiches kann gelten, wenn personenbezogene Daten infolge eines früheren Leaks[24] bereits der Kontrolle des Betroffenen bzw. Anspruchstellers entzogen wurden und die Daten von unbestimmten Dritten bereits vor einem neuen Datenschutzvorfall zur Kenntnis genommen werden konnten.

Dr. Sascha Vander

LL.M., RA und FA für IT-Recht bei CBH Rechtsanwälte, Cornelius Bartenbach Haesemann & Partner (Köln) im Bereich IP/IT. Schwerpunkte: IT-Projekte, Software- und Lizenzrecht, E-Commerce, Wettbewerbs-, Medien- und Datenschutzrecht. 2005 Promotion zum Thema Mehrwertdienste. 2007 LL.M. (Informationsrecht).

20 Siehe OLG München, 13. 2. 2025 – 24 U 3020/24 e, juris; OLG Dresden, 11. 2. 2025 – 4 U 1283/24, juris; siehe auch OLG Düsseldorf, 14. 3. 2025 – I-16 U 94/24, im Ergebnis allerdings mit der Annahme eines hinreichend substantiierten Kontrollverlusts.

21 OLG Dresden, 21. 1. 2025 – 4 U 738/24, Rn. 20, juris.

22 OLG Schleswig, 16. 10. 2024 – 5 U 56/24, WRP 2025, 253.

23 Vgl. OLG Dresden, 10. 12. 2024 – 4 U 808/24, Rn. 28, K&R 2025, 133; OLG Düsseldorf, 14. 3. 2025 – I-16 U 184/23, Rn. 28, 29, juris.

24 Vgl. die betreffenden Kontrollüberlegungen des OLG Dresden, 21. 1. 2025 – 4 U 738/24, Rn. 21, juris.

RA Prof. Dr. Jens M. Schmittmann und Prof. Dr. Julia Sinnig*

Update: Besteuerung der digitalen Wirtschaft 2024/2025 – Teil 2

Entwicklungen im Steuerrecht in der Informationstechnologie

Kurz und Knapp

Die Autoren fassen in diesem zweiteiligen Beitrag die aktuellen steuerrechtlichen Entwicklungen des vorangehenden Jahres zusammen, sofern sich Bezüge zur Informationstechnologie im weitesten Sinne und dem Informationstechnologierecht ergeben. Teil zwei legt den Fokus auf das deutsche Recht. Der Beitrag fasst die wesentlichen Entwicklungen in Legislative und Judikative bei der Besteuerung der digitalen Wirtschaft in Deutschland zusammen.[1]

* Mehr über den Autor und die Autorin erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 5. 4. 2025.

1 Vgl. *Schmittmann/Sinnig*, K&R 2023, 100 ff., 178 ff.; *dies.*, K&R 2022, 87 ff., 175 ff.; *dies.*, K&R 2021, 92 ff., 164 ff.; *dies.*, K&R 2020, 111 ff., 183 ff.; *dies.*, K&R 2019, 88 ff., 158 ff.; *Schmittmann*, K&R 2018, 19 ff.; *ders.*, K&R 2017, 157 ff.; *ders.*, K&R 2016, 28 ff.