48. Jahrgang
datenschutz-berater.de
DSB 12/2024

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Prof. Christian Solmecke

BGH zum Facebook-Datenleck: Das Beste kommt zum Schluss

BGH, Urt. v. 18.11.2024 – VI ZR 10/24

Die Gerichtsentscheidung in Kürze

Das Beste kommt zum Schluss. So lässt sich die vorliegende Entscheidung im Fall des Facebook-Datenlecks wohl treffend zusammenfassen. Nicht nur, dass sie den vorläufigen Abschluss von tausenden Zivilverfahren in Deutschland bietet; vielmehr setzt sich der Bundesgerichtshof erstmalig intensiv mit Unterlassungsansprüchen, Feststellungsansprüchen und Auskunftsansprüchen der Betroffenen eines Datenlecks auseinander und gibt zum Schluss auch noch Hinweise für die Berechnung von immateriellen Schadensersatzansprüchen nach Art. 82 DSGVO.

Der Fall

Hintergrund dieses Verfahrens ist ein gigantisches Datenleck, in dessen Folge im April 2021 Daten von weltweit 533 Millionen Nutzern veröffentlicht worden sind. Sechs Millionen deutsche Facebook-Kunden waren von der illegalen Ausnutzung der Kontaktimportfunktion des Netzwerkes betroffen. Allein beim Verfasser dieses Aufsatzes meldeten sich weit über 200.000 Betroffene und daraus resultierten über 4.300 Gerichtsverfahren. Der Vorwurf: Facebook hat u. a. durch seine Voreinstellungen mehrfach gegen die DSGVO verstoßen und so dazu beigetragen, dass Scraper die Daten abgreifen konnten. Deshalb schuldet das Netzwerk den Betroffenen immateriellen Schadensersatz nach Art. 82 Abs. 1 DSGVO.

Waren die deutschen Gerichte den Klageverfahren anfangs noch sehr positiv gegenüber eingestellt und sprachen analog zur bisherigen Rechtsprechung bei Datenschutzverstößen noch Schadensersatzsummen in Höhe von bis zu 1.000 Euro aus, kippte die Stimmung mit der zunehmenden Anzahl der Verfahren, die manche Richter nur noch als lästig bezeichneten. Das gipfelte darin, dass die Oberlandesgerichte fast unisono – und entgegen den klaren Vorgaben des EuGH – in dem durch das Datenleck entstandenen Kontrollverlust schon keinen Schaden sahen – oder, wenn überhaupt, nur einen immateriellen Schaden im einstelligen Euro-Bereich annehmen wollten. Deutlich sichtbar wurde diese Mentalität der Gerichte am 18. November 2024, dem Tag der Urteilsverkündung: obwohl klar war, dass die schriftlichen Urteilsgründe des BGH binnen weniger Tage veröffentlicht werden würden, ergingen noch zahlreiche klageabweisende Entscheidungen am Ende der Sitzung. Man wollte die lästigen Verfahren, an denen sich mutmaßlich nur die Rechtsanwälte bereicherten, schnell noch vom Tisch haben, bevor das höchste deutsche Zivilgericht möglicherweise eine andere Entscheidung treffen würde.

Die Gründe

Die Vorahnung schien zu passen. Zum Schadenersatz stellte der BGH – so wie auch der EuGH (zuletzt Urt. v. 4.10.2024 – C-200/23) – fest, dass die Betroffenen eines Datenlecks schon allein deswegen einen Anspruch auf Erstattung eines immateriellen Schadenersatzes haben, weil sie die Kontrolle über ihre Daten verloren haben. Dies ergebe sich aus dem eindeutigen Wortlaut des ErwGr. 85 zur DSGVO. Betroffene müssten – anders als es noch die Vorinstanz sagte – nicht darlegen, unter sich daraus entwickelnden besonderen Befürchtungen oder Ängsten zu leiden; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern.

Grundsätzlich stellt der BGH auch nicht in Abrede, dass im konkreten Fall ein solcher Kontrollverlust stattgefunden hat. Bei der öffentlichen Preisgabe der Telefonnummer, die die Betroffenen nicht willentlich der Öffentlichkeit preisgeben wollten, lag das auf der Hand. Auch bei abgegriffenen öffentlichen Daten wie Name, Geschlecht und Nutzer-ID kann nach Einschätzung des 6. Zivilsenats ein Schaden entstanden sein. Allerdings muss die Vorinstanz nun prüfen, ob die Nutzer nicht durch die Zustimmung zu den Nutzungsbedingungen des Netzwerks in die unbedingte Veröffentlichung ihrer Daten wirksam eingewilligt haben. Der BGH gibt dem OLG in den Urteilsgründen jedoch entsprechende Hinweise, aufgrund welcher Vorgaben der DSGVO eine entsprechende Einwilligung unwirksam gewesen sein könnte (u. a. Transparenz, Freiwilligkeit und marktbeherrschende Stellung von Meta).

Anwaltskosten für ein außergerichtliches Tätigwerden hielten etliche deutsche Gerichte schon nicht für ersatzfähig. Dazu stellte der BGH nun fest, dass die Verfahren eine Vielzahl von ungeklärten Rechtsfragen beinhalten und die Einschaltung eines Rechtsbeistandes durchaus vonnöten sein könne. Die vorgerichtlichen Anwaltskosten sieht der BGH daher klar als Schaden im Sinne von Art. 82 DSGVO.

Ebenfalls als zulässig erachtete der BGH den Feststellungantrag dahingehend, dass Meta künftige materielle sowie

derzeit noch nicht vorhersehbare immaterielle Schäden ersetzen muss. Der Antrag sei konkret genug. Zudem bestehe, solange die Daten des Klägers im Internet öffentlich sind, weiterhin das Risiko einer missbräuchlichen, insbesondere betrügerischen Nutzung dieser Daten mit der Folge eines materiellen oder immateriellen Schadens.

Schließlich bejaht der BGH einen Unterlassungsanspruch dahingehend, dass Facebook die Mobiltelefonnummer des Klägers nicht mehr verarbeiten darf, soweit dies über die Nutzung der Zwei-Faktor-Authentifizierung hinausgeht.

Keine Vorlage an den EuGH

Mit Spannung erwartet wurde die Frage, ob der BGH erneut offene Fragen dem EuGH zur Vorabentscheidung vorlegen würde. Er hat sich dagegen entschieden. Ob der Kontrollverlust allein einen Schaden darstellt, steht für den BGH aufgrund der insoweit eindeutigen EuGH-Rechtsprechung unzweifelhaft fest. Sofern der Senat bereits zuvor die Frage vorgelegt hatte, ob ein Unterlassungsanspruch aus nationalem Recht neben fehlenden Unterlassungsansprüchen in der DSGVO Raum hat, so hielt er diese Frage hier noch nicht für entscheidungserheblich. Es könne sein, dass das OLG in der erneuten Verhandlung feststellt, dass hier auch ein Unterlassungsanspruch aus dem Facebook-Nutzungsvertrag selbst existiere. Dann könne die Frage offenbleiben, ob trotz fehlendem Unterlassungsanspruch in der DSGVO die nationalen Normen aus § 1004 Abs. 1 Satz 2 i. V. m. § 823 BGB zur Anwendung kommen. An dieser Stelle wäre es nach Meinung des Verfassers erwähnenswert gewesen, dass sich der EuGH jüngst in seiner Entscheidung vom 4. Oktober genau zu einer solchen Frage geäußert hat. Dort ging es darum, ob nationale wettbewerbsrechtliche Ansprüche, die auf das Unterlassen von Datenschutzverstößen gerichtet sind, anwendbar sind. Die Frage wurde vom EuGH klar bejaht; warum das bei Unterlassungsansprüchen, die sich aus Verletzung des allgemeinen Persönlichkeitsrechts ergeben, anders sein sollte, ist nicht ersichtlich.

Der Senat hatte in einer seiner früheren Vorabvorlagen den EuGH außerdem gefragt, ob Sorgen und Ängste über den Missbrauch von Daten allein einen Schadenersatzanspruch begründen können. Hier hielt er diese Frage nicht für entscheidungsrelevant, da es jedenfalls einen Kontrollverlust gibt, der für sich genommen schon einen Schadenersatzanspruch begründet. Ängste und Sorgen allein aber würden alternativ bereits ausreichen, um einen immateriellen Schaden darzustellen, selbst wenn kein Kontrollverlust nachgewiesen werde. Kämen Kontrollverlust und Ängste zusammen, würde dies den Schadenersatzanspruch aber erhöhen.

Auch wenn die Frage, ob Facebook hier überhaupt einen Datenschutzverstoß begangen hat, nicht vom BGH zu klären war, so bejaht er diese jedoch mit deutlichen Worten. Damit liegt er auf der Linie nahezu aller deutscher Gerichte und auch auf der Linie der irischen Datenschutzkommission, die am 25. November 2022 ein Bußgeld in Höhe von 265 Millionen Euro wegen des Datenlecks gegen den Meta-Konzern verhängte. Nach Meinung des Senats dürfte die Voreinstellung in der Facebook-Suchbarkeit auf „für alle“ dem Grundsatz der Datenminimierung widersprechen, Art. 5 Abs. 1 lit. c DSGVO. Und auch die sonstigen Voreinstellungen für den Nutzer sah er im Sinne von Art. 25 Abs. 2 DSGVO nicht als sonderlich datenschutzfreundlich an. Es liegt in der Natur der Sache, dass ein soziales Netzwerk gerne die Daten der Nutzer möglichst öffentlich machen möchte. Das widerspricht allerdings Art. 25 DSGVO, der genau in solchen Fällen soziale Netzwerke zu datenschutzfreundlichen Voreinstellungen verpflichtet, da der Nutzer werkseitige Voreinstellungen nur selten verändert.

Kriterien für DSGVO-Schadensersatz

Ebenfalls mit Spannung erwartet wurden die Ausführungen des BGH zur Berechnung des Schadenersatzes. Einleitend stellt der BGH noch einmal die Ausführungen des EuGH dar, wonach die DSGVO keine Anhaltspunkte für die Berechnung vorsieht und die Bußgeldnormen aus Art. 83 DSGVO eine andere Intention haben. Insofern müssen nationale Gerichte den Schaden nach § 287 ZPO ermitteln, so nun der BGH. Dabei müssen aber einige unionsrechtliche Vorgaben beachtet werden: Die Ausübung der Rechte darf den Nutzern nicht unmöglich gemacht werden; die Entschädigung muss vollständig und wirksam sein, um den Schaden in vollem Umfang auszugleichen, wobei eine Abschreckungs- oder Straffunktion abgelehnt wird; wie oft der Betroffene von dem Verstoß getroffen wird, muss unberücksichtigt bleiben. Wenn der Schaden gering ist, soll auch nur ein Schadenersatz in geringer Höhe zuzusprechen sein, sagt der BGH und folgt damit den Vorgaben des EuGH im Urteil vom 4. Oktober 2024. Dort hatten die Luxemburger Richter klar herausgestellt, dass der durch die Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung.

Folgt man dieser Argumentation des EuGH, erscheint ein immaterieller Schadenersatzanspruch im vier- oder sogar fünfstelligen Bereich eigentlich durchaus möglich. Das sah der BGH nun teilweise anders – zumindest sofern nur der bloße Kontrollverlust der eigenen personenbezogenen Daten kompensiert werden soll. Doch bevor er konkrete Zahlen nennt, stellt der Senat zunächst einmal fest, wie der Tatrichter bei der Schadensschätzung vorgehen kann. Er stellt dabei auf einen Fall ab, bei dem der Schaden allein im Kontrollverlust liegt und sonstige schadenerhöhende Kriterien wie Ängste, Sorgen oder psychische Beeinträch-

tigungen nicht hinzukommen. Liegt der Schaden allein im Kontrollverlust, muss zunächst die Sensibilität der konkret betroffenen Daten betrachtet werden. Es liegt auf der Hand, dass Gesundheitsdaten sensibler sind als der Vorname einer Person. Darüber hinaus fällt auch ins Gewicht, wie die betroffenen Daten typischerweise verwendet werden. Der Schaden erhöht sich, wenn der Kontrollverlust dauerhaft ist und die Möglichkeit der Wiedererlangung der Kontrolle nicht besteht. Ebenfalls schadenerhöhend sieht es der BGH an, wenn unbegrenzt viele Empfänger die gestohlenen Daten abrufen können.

Hier sieht der BGH den Kontrollverlust zwar als dauerhaft an. In seinen Augen kann die verlorengegangene Kontrolle über die Handynummer aber dadurch wiedererlangt werden, indem man die Handynummer wechselt. Und genau diesen Wechsel der Handynummer bepreist er – ohne nähere Ausführungen – mit mindestens 100 Euro und liegt damit auf einer zuvor schon geäußerten Linie des OLG Hamm. Eine klare Absage wird allerdings der Meinung des OLG Celle erteilt, das hier nur einen Schadenersatz im einstelligen Euro-Bereich gesehen hat.

Auswirkungen auf die Praxis

Es wird jetzt Aufgabe der nationalen Gerichte sein, im Einzelfall zu bemessen, ob die 100 Euro wirklich für die Schadenkompensation ausreichen werden. Sollten Betroffene bereits in der Vergangenheit durch Hunderte SMS, die auf das Datenleck zurückzuführen sind, belästigt worden sein oder Telefonanrufe von unbekannten Dritten erhalten haben, dürfte der Anspruch auch deutlich höher ausfallen. Gleiches gilt auch für Handynummern von Prominenten, die ebenfalls haufenweise im Datenleck vorhanden waren. Schließlich ist es eindeutig als schadenserhöhend zu werten, wenn Betroffene glaubhaft vortragen können, aufgrund des Vorfalls unter begründeten Befürchtungen vor Missbrauch ihrer Daten zu leiden.

Jeder kann sich nun selbst fragen, ob es angemessen ist, den Wechsel einer liebgewonnenen Handynummer mit 100 Euro zu bepreisen oder nicht. Vermutlich wären viele Menschen in Deutschland bereit, deutlich mehr Geld dafür auszugeben, dass sie ihre Handynummer, die vielleicht schon seit Jahrzehnten genutzt wird, behalten dürfen. Dem Verfasser dieses Textes wäre seine eigene Handynummer jedenfalls deutlich mehr wert – sie ist übrigens ebenfalls im Facebook-Datenleck zu finden und leider unwiderruflich „verbrannt". Und auch der vorsitzende Richter des 6. Zivilsenats äußerte in der mündlichen Verhandlung, dass er es gar nicht gerne sähe, wenn seine Handynummer im Internet veröffentlicht worden wäre. Sonderlich dramatisch scheint der Senat die Veröffentlichung dann aber doch nicht zu sehen, wenn am Ende 100 Euro für die Kompensation des Schadens regelmäßig ausreichen sollen. Hier bleibt abzuwarten, wie die unteren Instanzen diese Vorgaben des höchsten deutschen Zivilgerichts künftig mit Leben füllen werden.

Handlungsanweisung für die Praxis/Fazit

Nachdem der BGH nach den klaren Vorgaben des EuGH jetzt gar nicht mehr anders konnte, als den Kontrollverlust als Schaden anzuerkennen, dämmt er denkbare neue Klagewellen über eine deutliche Reduktion der Schadenshöhe ein. Betroffene werden wegen eines Schadens in Höhe von 100 bis 500 Euro vermutlich nicht die Mühen eines über mehrere Instanzen dauernden Gerichtsverfahrens auf sich nehmen.

Aber es ist genauso klar, dass hier Lösungen für die Betroffenen geschaffen werden müssen, die unabhängig von der Frage sind, ob die Opfer eines Datenlecks über eine Rechtsschutzversicherung oder nicht verfügen. Solche Lösungen werden schon jetzt angeboten: Prozessfinanzierer kaufen die Schadensersatzansprüche im Fall des Twitter- oder Facebook-Datenlecks für Preise zwischen 20 und 25 Euro und setzen diese dann gebündelt und im eigenen Namen durch. Darüber hinaus gibt es Alternativen, bei denen Prozessfinanzierer die gesamten Prozesskosten für den Betroffenen übernehmen und nach dem „Flightright"-Modell nur bei Erfolg eine Provision in Höhe von 25 Prozent erhalten. Diese Lösung wird die Gerichte entlasten und trotzdem dafür sorgen, dass die Betroffenen eine angemessene Entschädigung erhalten. Die Prozessfinanzierer hatten sich hier bislang noch bedeckt gehalten, da die Frage, ob der Kontrollverlust über die Daten einen Schadenersatzanspruch begründet, bislang in Deutschland nicht geklärt war. Das ist nun anders. Insofern stellt dieses Urteil nicht das Ende der Klagen in Sachen Datenlecks dar, sondern den Anfang.

Autor: **Christian Solmecke ist Rechtsanwalt und Partner der Kölner Rechtsanwaltskanzlei WBS.LEGAL, die sich u. a. auf das Medien-, Internet- und Datenschutzrecht spezialisiert hat. Der Autor vertritt in dem dem Urteil zugrundeliegenden Verfahren die Klägerseite.**