NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

7 / 2023
Juli 2023

Der Zweck heiligt die Mittel?

Zulässigkeit und Grenzen des White Hat Hackings

Cheat happens

Vorlage an den EuGH zur urheberrechtlichen Zulässigkeit von Cheat-Software

Aus die Maus?

Das Urheberrecht an Micky Maus läuft in den USA Ende 2023 aus – ein Überblick zum internationalen Urheberrecht

Kurzbeitrag: Nicht (un)erheblich!

Das Urteil des EuGH zum immateriellen Schadensersatz nach der DSGVO

Der Zweck heiligt die Mittel?

Zulässigkeit und Grenzen des White Hat Hackings

von Johanna Voget

Hacking und Cyberattacken sind aus dem Alltag und der medialen Berichterstattung nicht mehr wegzudenken. Zahlreiche Unternehmen und Institutionen hierzulande sind inzwischen Opfer eines solchen Angriffs geworden und haben mit den Folgen zu kämpfen. Die Forschungsstelle Recht berichtete im DFN-Infobrief Recht bereits in der Vergangenheit zu rechtlichen Fragestellungen rund um Cyberangriffe.[1] Eine Möglichkeit, Sicherheitslücken im System ausfindig zu machen und sich so besser vor Attacken schützen zu können, ist das sog. White Hat Hacking. Dieser Beitrag widmet sich der rechtlichen Bewertung solcher simulierten Angriffe.

I. Einleitung

Auch für Hochschulen und andere öffentliche Einrichtungen ist die ständige Angst vor einem Cyberangriff zur Realität geworden. Ein prominentes Beispiel der aktuellen Angriffe ist das Phänomen „Ransomware". Darunter ist eine Schadsoftware zu verstehen, die auf die Blockade des Computersystems oder die Verschlüsselung der Betriebs- und Nutzerdaten abzielt. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt.
Doch wie lassen sich solche Angriffe vermeiden?
Grundsätzlich ist jedes Unternehmen gem. Art. 32 Abs. 1 Datenschutzgrundverordnung (DSGVO) verpflichtet, angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu treffen und durch technische und organisatorische Vorkehrungen sicherzustellen, dass ihre Telemedienangebote gesichert sind, vgl. § 19 Abs. 4 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).

Die Einführung und Aufrechterhaltung angemessener Informationstechnik (IT)-Sicherheitsmaßnahmen ist jedoch eine hochkomplexe Aufgabe, die eine umfassende Kenntnis und ständige Überprüfung der eingesetzten IT-Infrastruktur voraussetzt.
Beispiele für Maßnahmen zur Qualitätssicherung der IT sind unter anderem Code-Reviews, SDL (Security Development Lifecycle von Microsoft) oder Grundschutz- und ISO-Zertifizierungen.
Eine andere (und wohl noch bessere) Möglichkeit, um mehr Cyber-Sicherheit zu erreichen, ist aber – ironischerweise – das Hacking selbst. Unter dem Terminus „White Hat Hacking" versteht man eine ethische Form des Hackings, die nicht dazu dienen soll, natürlichen oder juristischen Personen Schaden zuzufügen. Vielmehr werden durch Reverse Engineering und sog. „Penetrationtests" potenzielle Angriffsszenarien simuliert, um so mögliche Einfallstore für Angreifer zu identifizieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt sogar, dass bei Anwendungen und IT-Systemen mit erhöhtem Schutzbedarf Penetrationstests durchgeführt werden sollten.[2]
Mit ihren Angriffen setzen sich die White Hat Hacker jedoch einem straf- und datenschutzrechtlichen Risiko aus.
Was muss im Rahmen des Hacks also beachtet werden? Darf jeder ungefragt Penetrationtests vornehmen und in welchem Umfang?

1 Uphues, Der Feind in meinem Netz – Teil 1, DFN-Infobrief Recht 01/2020; Uphues, Der Feind in meinem Netz – Teil 2, DFN-Infobrief Recht 02/2020.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3 5 [Stand vom 08.05.2023].

II. Strafbarkeit des White Hat Hackings

1. Ausspähen von Daten

Nach § 202a Strafgesetzbuch (StGB) macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

Dem Begriff der „Daten" ist ein weites Verständnis zugrunde zu legen. Erfasst sind daher jede Art von Informationen und Programmen. Die Daten müssen jedoch elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein oder übermittelt werden.[3]

Nicht für den Täter bestimmt sind Daten, die nach dem Willen des Berechtigten nicht in den Herrschaftsbereich des Täters gelangen sollen. Der Verfügungsberechtigte ist grundsätzlich der, der zum Zeitpunkt der Tat die Verfügungsmacht über die Daten innehat. In der Regel wird die Verfügungsmacht beim erstmaligen Erstellen der Daten mit dem Abspeichern (sog. Skripturakt) begründet. Es kommt also nach herrschender Meinung nicht auf den Besitz oder das Eigentum am Datenträger an.[4]

Des Weiteren sind vom Schutz des § 202a StGB nur Daten erfasst, die „gegen unberechtigten Zugang" gesichert sind. Der Täter muss also eine Zugangssicherung, beispielsweise Passwörter oder Schreib- und Leseberechtigungen, überwunden haben.

An diesem Merkmal entzünden sich praktische Fragen: Wann genau ist ein Schutz gegen unberechtigten Zugang anzunehmen? Teilweise wird dieses Merkmal denkbar weit verstanden: der Zugang für eine Person sei immer dann unberechtigt, wenn die Daten nicht für sie bestimmt sind.

In der Realität sind die Systeme jedoch teilweise so schlecht „gesichert", dass sie aus informationstechnischer Sicht nicht als „besonders geschützt" gelten können. Muss also keinerlei Zugangssicherung überwunden werden, kann auch keine Strafbarkeit gem. § 202a StGB in Betracht kommen. Zu diesem Ergebnis kam das Landeskriminalamt Berlin auch im Fall der White Hat Hackerin Lillith Wittmann und der Wahlkampf-App „CDU Connect". Die Daten seien hier aus „technischer Sicht öffentlich abrufbar" gewesen.[5]

Besonders problematisch stellen sich in diesem Zusammenhang interne Arbeitnehmerfälle dar: Dringt ein Unternehmen im Rahmen eines Penetrationstests berechtigt in sein eigenes, gesichertes System ein, wo sich jedoch (weisungswidrig) abgelegte, unverschlüsselte, private Arbeitnehmerdaten befinden, so soll ein unberechtigter Zugang vorliegen.[6]

Darüber hinaus muss der Täter unbefugt handeln. Dies bedeutet im Gegenzug, dass das Handeln mit Einverständnis des Verfügungsbefugten die Tatbestandsmäßigkeit entfallen lässt. Der Gesetzgeber hat selbst in der Begründung zur Neufassung des § 202a StGB hervorgehoben, dass das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens nicht strafbar sei, sofern der Hacker von dem Unternehmen mit dieser Aufgabe betraut worden ist.[7] Auch der Erwägungsgrund 17 der EU-Richtlinie zur Cyberkriminalität[8] macht deutlich, dass mangels Vorsatz keine strafrechtliche Verantwortung begründet wird, wenn Personen beauftragt werden die Sicherheit von IT-Systemen zu testen. Vertragliche Vereinbarungen zur Beschränkung des Zugangs zu Informationssystemen des zu prüfenden Unternehmens sollen mithin keine Strafbarkeit des testenden Dienstleisters nach sich ziehen.

Das mag auf den ersten Blick so klingen, als sei das White Hat Hacking damit entschärft und jedes Strafbarkeitsrisiko ausgeschlossen.

Dem ist jedoch nicht so. Weiterhin soll nämlich Unternehmen am Quellcode der von ihnen in der IT-Struktur eingesetzten Standardsoftware oder an den (weisungswidrig) von Arbeitnehmern gespeicherten Daten die Verfügungsbefugnis fehlen.[9]

---

3 BeckOK StGB/Weidemann StGB § 202a Rn. 5.

4 BeckOK StGB/Weidemann StGB § 202a Rn. 9.

5 https://netzpolitik.org/2022/hackerparagrafen-sicherheit-fuer-die-sicherheitsforschung/ [Stand vom 08.05.2023].

6 Kipker/Rockstroh, ZRP 2022, 240 (241).

7 https://dserver.bundestag.de/btd/16/036/1603656.pdf (S. 10) [Stand vom 08.05.2023].

8 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2013:218:FULL&from=FI [Stand vom 08.05.2023].

9 Kipker/Rockstroh, ZRP 2022, 240 (241); siehe zu den Zugriffsbefugnissen des Systemadministrators: John, Error 403. Zugriff verweigert., DFN-Infobrief Recht 03/2021

Teilweise werden auch externe Sicherheitstester aufgrund der expliziten vertraglichen Vereinbarungen anders behandelt als interne Tester.

Zwar hat der Gesetzgeber das Strafrechtsrisiko wohl mittlerweile erkannt. So ermächtigt § 7a Abs. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) das BSI, auf dem Markt bereitgestellte IT-Produkte zu untersuchen, um Sicherheitsinformationen zu beschaffen, handelnde Behördenmitarbeiter werden also nunmehr geschützt. Es fehlt aber bis heute an einer ausdrücklichen Berechtigung für privatrechtliche Penetrationstester.

2. Vorbereiten des Ausspähens und Abfangens von Daten

Nach § 202c StGB macht sich auch strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, sich oder einem anderen verschafft.

Nach der Begründung des Gesetzgebers soll hierbei lediglich das Herstellen, Verschaffen, Verbreiten usw. solcher Programme, denen die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind, unter Strafe gestellt werden. Bei Programmen, deren primärer Zweck nicht klar erkennbar ein krimineller ist (z. B. bei Sicherheitsüberprüfungen oder im Forschungsbereich) werden (sog. „dual use tools"), soll der Tatbestand hingegen nicht erfüllt sein.[10] Klare Vorgaben für die Praxis lassen sich daraus jedoch nicht entnehmen, sodass allgegenwärtige Unsicherheiten verbleiben, welche Programme nun genutzt werden dürfen und welche nicht.

III. Datenschutzrechtliche Risiken

1. Verarbeitung personenbezogener Daten durch Penetrationtests

Zunächst ist zu prüfen, ob durch die Penetrationtests überhaupt personenbezogene Daten iSv Art. 4 Nr. 2 DSGVO verarbeitet werden. Jedenfalls ausgeschlossen werden kann eine Datenverarbeitung immer dann, wenn der Test vollständig anhand künstlich erzeugter Testdaten durchgeführt wird. Wird jedoch ein „Live"-System getestet, ist das Vorliegen einer Verarbeitung konkret zu prüfen.[11] Problematisch ist darüber hinaus, dass im Vorfeld der Durchführung des White Hat Hackings in der Regel nicht feststeht, ob dabei auf personenbezogene Daten zugegriffen wird. In Gestalt der „anderen Form der Bereitstellung" gem. Art. 4 Nr. 2 DSGVO kommt es auch nicht darauf an, ob die personenbezogenen Daten vom Hacker dann tatsächlich zur Kenntnis genommen, also ausgelesen oder gespeichert werden. Vielmehr begründet schon die reine Zugriffsmöglichkeit durch den Dritten das Vorliegen einer Verarbeitung. Genau diese Möglichkeit des Zugriffs zu überprüfen und zu testen ist ja aber wiederum grade Zweck des White Hat Hackings.
Daraus folgt auch, dass zum Zeitpunkt der Beauftragung des Hackers noch nicht absehbar ist, ob der Abschluss einer Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO erforderlich ist oder nicht. Die Relevanz dieser Frage ergibt sich daraus, dass der Auftragsverarbeiter selbst keiner Rechtsgrundlage für eine Verarbeitung bedarf, sondern sich vielmehr auf die Rechtsgrundlage stützen kann, die dem Verantwortlichen die Verarbeitung gestattet. Für die Abgrenzung der Auftragsverarbeitung von der eigenständigen Verantwortlichkeit ist im Einzelfall insbesondere der Grad der Weisungsgebundenheit des Hackers zu prüfen.[12]

2. Erlaubnistatbestände

Aufgrund ihrer Widerruflichkeit ist die Einwilligung der Betroffenen gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO zur Durchführung von Penetrationtests als untauglich anzusehen.[13]

---

10 https://dserver.bundestag.de/btd/16/036/1603656.pdf (S. 18 f.) [Stand vom 08.05.2023].

11 Poncza, ZD 2023, 8 (9).

12 Poncza, ZD 2023, 8 (9).

13 Poncza, ZD 2023, 8 (10).

In Betracht kommt vielmehr eine Rechtmäßigkeit der Verarbeitung aufgrund eines berechtigten Interesses nach Art. 6 Abs. 1 S. 1 lit. f DSGVO.

Der Erwägungsgrund 49 zur DSGVO sieht hierzu vor, dass die Sicherheit von IT-Systemen des Verantwortlichen und der Schutz vor Angriffen ein berechtigtes Interesse begründen kann. Inwieweit die Durchführung von Penetrationtests im Rahmen einer Interessenabwägung zu einem überwiegenden Interesse des Verantwortlichen führt, muss jedoch stets im Einzelfall gesondert geprüft werden, sodass eine erhebliche Rechtsunsicherheit verbleibt.

Zudem ist zu berücksichtigen, dass unter Umständen auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet werden und für die Begründung der Zulässigkeit von Hackingangriffen bezogen auf solche Daten erhöhte Anforderungen zu erfüllen sind.

Im Forschungs- und Wissenschaftsbereich kommt hier § 27 BDSG als Grundlage der Datenverarbeitung in Betracht. Darüber hinaus wird eine Rechtsgrundlage nur in Art. 9 Abs. 2 lit. g DSGVO i.V.m. Art. 32 Abs. 1 lit. d DSGVO gesehen.[14]

IV. Schutzpflicht des Staats und Handlungsbedarf

Das Bundesverfassungsgericht (BVerfG) selbst hat aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme abgeleitet.[15]
Hiernach trifft den Staat auch eine Pflicht, dazu beizutragen, „dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt werden".[16]

White Hat Hacking trägt zum Schutz informationstechnischer Systeme bei, aber den Durchführenden drohen nach der derzeitigen Rechtslage schwerwiegende Konsequenzen. Daher dürfte den Staat unter Anwendung des Rechtsprechung des BVerfG grundsätzlich auch die Pflicht treffen, durch die Einführung tatbestandsausschließender Regelungen im Cyberstrafrecht die rechtlichen Rahmenbedingungen zur risikofreien Durchführung von Penetrationstests zu schaffen.[17]

Die Ampelregierung hat es sich im Koalitionsvertrag zur Aufgabe gemacht, die IT-Sicherheit zu stärken, indem „das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, beispielsweise in der IT-Sicherheitsforschung, legal durchführbar" werden soll.[18]

Darüber hinaus haben sich Expertengruppen beraten und in einem Whitepaper die Probleme und den Handlungsbedarf aufgezeigt sowie konkrete Regelungsvorschläge unterbreitet. [19] Bislang sind jedoch keine Gesetzesinitiativen bekannt, die Rechtsunsicherheit bleibt also vorerst bestehen.

Die Europäische Union (EU) hat zuletzt mit der NIS-2 Richtlinie[20] einen weiteren Schritt im Bereich der Cybersicherheit getan, um Schwachstellen der bislang geltenden NIS Richtlinie auszubessern und auf die Zunahmen der weiter entwickelten Cyberangriffe zu reagieren.[21] Hierzu informierte der DFN-Infobrief Recht auch kürzlich ausführlich.[21] Die neue Richtlinie betrifft zwar nicht explizit die Voraussetzungen und Grenzen des White Hat Hackings bzw. seine straf- und datenschutzrechtliche Behandlung, macht aber beispielsweise zur Vorgabe, dass Hochschulen und Forschungseinrichtungen bei der Entwicklung, der Verbesserung sowie dem Einsatz von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur zu unterstützen sind.[21]

---

14 Poncza, ZD 2023, 8 (12).

15 BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, NJW 2008, 822.

16 BVerfG, Beschluss vom 8.6.2021 – 1 BvR 2771/18, NJW 2021, 3033.

17 https://netzpolitik.org/2022/hackerparagrafen-sicherheit-fuer-die-sicherheitsforschung/

18 Koalitionsvertrag, S. 13 [Stand vom 08.05.2023].

19 https://sec4research.de/assets/Whitepaper.pdf [Stand vom 08.05.2023].

20 Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L1535&from=DE [Stand vom 08.05.2023].

21 John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS? DFN-Infobrief Recht 04/2023.

V. Bedeutung für Hochschulen

Die erneute Aufforderung an den nationalen Gesetzgeber durch die NIS-2 Richtlinie könnte genutzt werden, um auch eine rechtssichere Durchführung von White Hat Hacking zu gewährleisten. Ohne das vorherige Einverständnis der Betreiber der zu überprüfenden IT-Systeme ist bislang ohne die Befürchtung straf- und datenschutzrechtlicher Konsequenzen kein White Hat Hacking möglich. Darüber hinaus sind im Einzelfall weitere Fallstricke zu beachten, sodass insbesondere interne Hacking-Maßnahmen auch nach vorheriger Ankündigung nur mit äußerster Vorsicht durchgeführt werden sollten.

Cheat happens

Vorlage an den EuGH zur urheberrechtlichen Zulässigkeit von Cheat-Software

von Klaus Palenberg

Der Bundesgerichtshof (BGH) hat dem Europäischen Gerichtshof (EuGH) mit Beschluss vom 23. Februar 2023 (Az. I ZR 157/21) Fragen zur urheberrechtlichen Einordnung von sogenannter Cheat-Software vorgelegt. Dabei geht es zum einen um die Frage, ob die durch die Cheat-Software bewirkten Änderungen im Programmablauf einen Eingriff in die Urheberrechte der Programmierenden darstellen. Zum anderen geht es im Anschluss an die erste Frage darum, ob diese Änderungen ihrerseits wiederum einen urheberrechtlichen Verstoß bewirken. Mit der Reichweite des urheberrechtlichen Schutzes von Computerprogrammen kann auch die Frage der Mitbestimmung durch deren Entwickelnde über die weitere Nutzung der Software verbunden sein. Große Brisanz könnte dies wiederum bei Entwicklungen von IT-Sicherheits-Produkten zum Schutz vor Cyperangriffen erhalten, da hier die Auswirkungen einer missbräuchlichen Nutzung besonders fatal sein können.

I. Der Hintergrund des Verfahrens

Der urheberrechtliche Schutz von Computerprogrammen ist europarechtlich durch die RL 2009/24/EG (Computerprogramm-RL) weitgehend einheitlich geregelt und in Deutschland mit den §§ 69a ff. Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG) umgesetzt. Allerdings sind diese Regelungen bislang wenig konturiert. Mit seinen Vorlagefragen trägt der BGH daher dazu bei, dass eine bislang ungeklärte, aber entscheidende Frage auf dem Gebiet der Softwareprogrammierung durch den EuGH geklärt werden wird.

Dahinter steht der generelle Zielkonflikt der Richtlinie. Auf der einen Seite soll ein angemessener Schutz für Programmierende bestehen, der dann auch Anreize für Investitionen in Entwicklungen von Software schafft. Auf der anderen Seite sollen aber auch Interaktionen zwischen verschiedenen Programmen, z. B. über Schnittstellen, möglich sein, um auch Innovationen von kleineren Unternehmen zu fördern. Vor diesem Hintergrund befassen sich die Vorlagefragen konkret mit der Reichweite des Schutzes eines Computerspiels vor Änderungen im Spielablauf durch Dritte.

II. Der Sachverhalt

Der ursprüngliche Fall liegt mittlerweile ca. zehn Jahre zurück. Damals vertrieb die Sony Computer Entertainment Europe Ltd. (Sony) die mobile Spielekonsole „PlayStationPortable“ (PSP) sowie Spiele hierfür. Unter diesen Spielen befand sich die Rennsimulation „Motorstorm Arctic Edge“. Während des Spielens dieses Computerspiels war die Nutzung eines „Turbos“ möglich, um kurzfristig eine größere Beschleunigungskraft zu haben. Dieser „Booster“ sollte vom Originalspiel her allerdings nur in beschränktem Ausmaße zur Verfügung stehen. Daneben konnten im Laufe des Spiels auch zusätzliche Fahrer freigespielt werden. Gesteuert wurde das Spiel über das an der Konsole angebrachte Steuerkreuz und weitere verschiedene Tasten.

Um diese Beschränkungen zu umgehen und um von Anfang an sämtliche Fahrer zur Auswahl zu haben, konnten sich Nutzende des Computerspiels eine zusätzliche Software namens „Action Replay PSP“ kaufen. Zudem wurde auch ein Zubehör samt Software namens „Tilt FX“ angeboten, welches die Steuerung der Konsole durch Bewegung im Raum ermöglichte. Diese Ergänzungsprodukte wurden jedoch nicht von Sony selbst vertrieben, sondern von einem Drittunternehmen.

Für die Steuerung der PSP durch Bewegung mittels „Tilt FX“ wurde ein Bewegungssensor, der an den Headset-Anschluss der PSP angeschlossen werden musste, sowie dazugehörende Software geliefert. Um diese Zusatzsoftware, ebenso wie die Software „Action Replay PSP“, nutzen zu können, musste die Konsole mit einem PC verbunden werden und in die PSP ein Memory Stick (digitales Speichermedium in Form einer Flash-Speicherkarte) eingelegt und mit der Zusatzsoftware beschrieben werden. Im Anschluss an diese Prozedur erschien nach Neustart der Konsole ein zusätzlicher Menüpunkt „Action Replay“ bzw. „Tilt FX“, welcher jeweils in der Originalversion von Sony nicht vorhanden war. Über diese zusätzlichen Menüs konnten bestimmte, im Originalspiel angelegte, Beschränkungen abgewählt werden, wie beispielsweise die Begrenzung des Boosters, oder die Bewegungssteuerung aktiviert werden. Abgesehen von diesen Änderungen lief das Spiel wie ohne Installation der Zusatzsoftware ab.

Grob gesprochen funktionierte die Software „Action Replay PSP“ in etwa so, dass sie dem Betriebssystem der Konsole vorspiegelte ein Update zu sein und sich so installieren ließ. Über diesen Weg erhielt sie dann Zugriff auf bestimmte geschützte Bereiche im Arbeitsspeicher, die eigentlich dem Originalspiel vorbehalten waren. In diesen Bereichen legte die Originalsoftware variable Daten ab, mit denen sie gewisse Status, wie etwa die Anzahl der Booster Nutzungen oder die bislang freigespielten Fahrer, festhielt. Bei Auswahl der Funktionen der Zusatzsoftware änderte das Programm diese Variablen so ab, dass die zur Freischaltung sämtlicher Fahrer notwendige Punktzahl erreicht war und die Booster-Nutzungen nicht mitgezählt wurden. Den Quellcode der Original-Software änderte die Zusatzsoftware hingegen nicht. Da durch die Zusatzsoftware im Originalspiel angelegte Beschränkungen umgangen werden konnten, wird in diesem Zusammenhang von „Cheat-Software“ gesprochen. Allerdings bestand in diesem Fall eine kleine Besonderheit. Die durch die Cheat-Software ermöglichten Spielerleichterungen waren grundsätzlich bereits im Originalspiel angelegt. So war die Nutzung des Turbos auch dort möglich, allerdings nicht unbegrenzt. Auch die Fahrer waren bereits vorgesehen, nur sollten sie erst im Laufe des Spiels „erspielt“ werden. Die Steuerung des Spiels erfolgte auch im Original über Eingabe durch die Nutzenden, allerdings durch Tastendruck und nicht durch Bewegung im Raum. Dies ist nicht bei jeder Cheat-Software so der Fall. Stattdessen gibt es auch Cheat-Software, die zusätzliche Elemente, die im Original nicht vorhanden sind, wie etwa vollkommen neue Rennstrecken oder –wagen, ergänzen. Inwieweit sich die Ausführungen des EuGH auch auf solche Cheat-Software übertragen lassen, hängt von der konkreten Beantwortung der Vorlagefragen ab.

III. Die Vorlagefragen

Das Vorabentscheidungsersuchen des BGH enthält zwei Fragen. Die erste Frage befasst sich mit dem Umfang des Schutzes eines Computerprogramms nach der Richtlinie. Die zweite Frage soll den Begriff der Umarbeitung eines Computerprogramms i.S.d. Art. 4 Abs. 1 Buchst. b der Computerprogramm-RL klären.
Der BGH versteht die Funktionsweise der Cheat-Software in diesem Fall so, dass das Originalprogramm an sich unverändert bleibt. Das Programm lädt unangetastet in den Arbeitsspeicher und wird dort selbst, sowie seine Befehle auch nicht verändert. Lediglich vom Programm bei der Ausführung im Arbeitsspeicher abgelegte variable Daten werden durch die Cheat-Software abgeändert. Die Programmbefehle an sich bleiben jederzeit aktiv und die innere Struktur wird nicht angetastet. Geändert werden demnach nur aus dem laufenden Spiel heraus generierte Daten im Arbeitsspeicher. Insoweit liegen dem Programm andere Werte zu Grunde als ohne Einsatz der Cheat-Software. Grundsätzlich laufen die Spiele aber genauso ab, wie sie ursprünglich programmiert wurden.
Allerdings verändert die Cheat-Software die im Spiel erzeugten Daten, wie Verbrauchsstand des Turbos, freigespielte Fahrer etc. Damit weicht der tatsächliche Spielverlauf mehr oder weniger geringfügig von dem von den Programmierenden vorgestellten Verlauf ab. Die dadurch vorgespiegelten Zustände, wie unverbrauchter Booster, sind dem Originalspiel aber grundsätzlich bekannt und können auch im regulären Spielverlauf eintreten. Damit stellte sich dem BGH die erste Frage, ob eine Abweichung des Programmablaufs durch die Änderung von im Arbeitsspeicher abgelegten Variablen ohne den Objekt- oder Quellcode anzutasten einen Eingriff in den Schutzbereich eines Computerprogramms bedeutet. Dabei betont der BGH, dass die Kategorien der Variablen, die durch die Cheat-Software berührt werden, bereits im Originalspiel angelegt waren und somit die innere Struktur des Spiels unangetastet bleibt. Inwieweit sich allerdings Abweichungen ergeben würden, hätte die Cheat-Software unbekannte Dinge hinzugefügt, wie etwa einen ganz neuen Rennwagen, bleibt offen.

Nach Art. 1 der Computerprogramm-RL und der Umsetzung in § 69a UrhG sind zwar sämtliche Ausdrucksformen eines Computerprogramms (Abs. 2 S. 1) und Programme in jeder Gestalt,

einschließlich des Entwurfmaterials (Abs. 1) geschützt. Aber Ideen und Grundsätze als Basis des Programms sind ausdrücklich nicht geschützt (Abs. 2 S. 2). Deshalb möchte der BGH im Grunde wissen, ob der von den Programmierenden geplante Spielablauf eine Ausdrucksform des Computerprogramms ist oder bloß die diesem zugrundeliegende Idee.

Sony hatte argumentiert, dass es gerade die Aufgabe des Computerspiels gewesen sei, „mit Hilfe eines dynamischen Spielablaufs ein unterhaltendes und herausforderndes Spielerlebnis zu erzielen." Basis dieses dynamischen Spielverlaufs seien dann die zuvor erzielten Ergebnisse der Spielenden, die in den Variablen im Arbeitsspeicher festgehalten würden. Nur durch das Zusammenwirken dieser variablen Daten mit den Programmbefehlen entstehe der von den Programmierenden vorgesehene Spielablauf. Das Erschöpfen des Boosters oder die sich im Laufe des Spiels ausweitende Fahrerauswahl seien das vom Urheber festgelegte Ergebnis des Computerprogramms, welches nur durch Rückgriff auf die variablen Daten im Arbeitsspeicher erzielt werde. Ohne diese Variablen könne das Programm nicht planmäßig ablaufen und das vorgegebene Spielerlebnis geboten werden.
Nach Ansicht des BGH allerdings soll das Ziel eines Computerspiels, einen unterhaltsamen Spielablauf zu bieten, bei der Bestimmung des Schutzbereichs keine Rolle spielen. Denn weder die Funktionalität eines Computerprogramms noch die Programmiersprache oder das verwendete Dateiformat seien Ausdrucksformen des Computerprogramms. Das Ergebnis der Nutzung eines Computerprogramms sei nicht geschützt, da sonst zum Schaden des technischen Fortschritts die Monopolisierung von Ideen drohe.

Bei Romanen als Werke der Literatur können neben der konkreten Textfassung auch der Gang der Handlung und die Ausgestaltung der Szenen schutzfähig sein. Sony hatte dies auf Computerprogramme so übertragen, dass auch das Programmkonzept als solches schutzfähig sein müsse. Auch dieser Ansicht erteilt der BGH eine Absage, da durch die Cheat-Software nicht die handlungsbestimmenden Elemente, sondern allein in beim Spielen vom Nutzer generierten Daten eingegriffen werde. Insoweit sei nicht der von den Programmierenden vorgestellte Gang der Handlung oder Ausgestaltung der Szenen, sondern lediglich deren Reihenfolge und Häufigkeit betroffen.

Sollte der EuGH diese erste Frage dennoch mit Ja beantworten und hier einen Eingriff in die Urheberrechte von Sony erkennen, möchte der BGH die Reichweite des Begriffs der Umarbeitung geklärt haben. Die Cheat-Software verletzte das Urheberrecht von Sony nämlich nur, falls auch eine zustimmungsbedürftige Handlung i.S.d. Art. 4 Abs. 1 Computerprogramm-RL bzw. § 69c UrhG vorlag. In diesem Fall kam allein eine Umarbeitung nach Art. 4 Abs. 1 Buchst. b Computerprogramm-RL bzw. § 69c Nr. 2 S. 1 UrhG in Betracht. Im Grunde zielt aber auch diese Frage auf den gleichen Kern ab. Auch hierbei geht es darum, ob es für die Annahme einer Umarbeitung ausreicht, dass in den Ablauf des Computerprogramms eingegriffen wird. Oder ob eine Umarbeitung voraussetzt, dass der Quell- oder Objektcode verändert wird.

IV. Einordnung der Entscheidung

Der BGH hat in seinem Beschluss klar zum Ausdruck gebracht, wie er die hier verwendete Cheat-Software einordnet. Er versteht die Funktionsweise so, dass sie das Originalspiel weitgehend unberührt lässt und allein Einfluss auf den Spielablauf und das –ergebnis nimmt. Da dies aber auch von den Eingaben der Spielenden abhängt und damit von den Nutzenden generierten Inhalten, sieht er hier kein urheberrechtliches Schutzbedürfnis. Die von dieser Cheat-Software betroffene PSP wird inzwischen nicht mehr von Sony vertrieben. Dennoch hat auch Sony ein großes Interesse an der Klärung der zugrundeliegenden Rechtsfragen. Denn zum einen stammen die Gewinne der Computerspielindustrie nicht mehr nur allein aus dem einmaligen Verkauf eines Spiels, sondern inzwischen mehr und mehr aus sogenannten In-Game-Käufen. Dabei werden im Laufe des Spiels kostenpflichtige Zusatzangebote verkauft, wie etwa neue Charaktere, Ausrüstungen oder Fertigkeiten. Für diese beim Nutzenden eintretenden Veränderungen im Spielablauf besteht entsprechend ein großes wirtschaftliches Interesse auf Seiten der Spieleentwickler an einem urheberrechtlichen Schutz. Sollte sich der EuGH, voraussichtlich Ende 2024, der Ansicht des BGH anschließen und diese Cheat-Software nicht als Urheberrechtsverletzung ansehen, ist fraglich, ob dann die durch In-Game-Käufe verursachten Änderungen im Spielablauf geschützt sind. Auch zur Umgehung dieser Beschränkungen werden bereits Alternativen zum Einsatz der von den Spieleanbietenden geforderten Geldsummen angeboten.

Zum anderen wird mit dieser Vorlage durch den BGH auch eine spannende Nuance des Urheberrechts für Computerprogramme adressiert. Es geht nämlich um nicht weniger als die Definition des Begriffs des Computerprogramms und wie er im Lichte der

Computerprogramm-RL auszulegen ist. Damit verbunden ist wiederum die Frage, inwieweit die Programmierenden einer Computersoftware bestimmen dürfen, wie ihre Software eingesetzt und verwendet wird.

Deren Beantwortung dürfte, neben dem kommerziellen Sektor, auch für viele Programmierende an wissenschaftlichen Einrichtungen von erheblicher Bedeutung sein und mit Spannung erwartet werden. Denn neben der Frage des generellen urheberrechtlichen Schutzes, stellt sich gerade bei wissenschaftlichen Forschungen auch häufig die Frage nach einer missbräuchlichen Nutzung der Forschungsergebnisse. So möchten viele Entwickelnde zumindest mitbestimmen dürfen, wie ihre Entwicklungen am Ende tatsächlich genutzt werden. Dies gilt natürlich auch im Bereich der Software-Entwicklung und hier ganz besonders in Hinblick auf Cybersecurity. Je nach Auslegung des EuGH, bestünde dieses Mitbestimmungsrecht bereits auf Grund des urheberrechtlichen Schutzes von Computerprogrammen oder müsste anderweitig, etwa durch entsprechende Lizenzvereinbarungen, eingeräumt werden.

Aus die Maus?

Das Urheberrecht an Micky Maus läuft in den USA Ende 2023 aus – ein Überblick zum internationalen Urheberrecht

Von Nicolas John

Mäuse begeistern in der Film- und Serienwelt schon viele Generationen jeden Alters. Zu denken sei an die Sendung mit der Maus, Speedy Gonzales, Tom und Jerry, Mrs. Brisby oder Stuart Little. Doch die wohl bekannteste Maus der Zeichentrickwelt dürfte Micky Maus sein, die ihren ersten Auftritt schon im Stummfilm „Plane Crazy“ hatte, aber erst mit dem Film „Steamboat Willie“ 1928 weltbekannt wurde. Schnell folgten weitere Filme, Serien, Comics und Merchandise in jeder erdenklichen Art und tatsächlich auch der Stern auf dem Hollywood Walk of Fame. Wirtschaftlich gesehen ist die Maus für Walt Disney demnach ein wichtiger Bestandteil des Unternehmens. Der Schutz von Micky Maus spielt daher eine bedeutende Rolle. Grund genug, um sich mit dem Urheberrecht und vor allem den Schutzfristen und der Gemeinfreiheit von Werken zu beschäftigten.

I. Urheberrecht in Deutschland

In Deutschland bestimmt das Urheberrechtsgesetz (UrhG), dass im Moment der Schaffung eines Werkes ein Urheberrecht an dem Werk für dessen Urheber entsteht. Hierfür braucht es keines weiteren formellen Akts wie einer Anmeldung oder Registrierung des Werks. Das Urheberrecht entsteht ohne weiteres Zutun.
Ein Werk im Sinne des UrhG liegt dann vor, wenn vier Bedingungen erfüllt sind: Es muss sich um eine persönliche Schöpfung handeln, also auf einer menschlich-gestalterischen Tätigkeit der schaffenden Person beruhen. Außerdem muss sie eine wahrnehmbare Formgestaltung haben. Das bedeutet, sie muss für die menschlichen Sinne wahrnehmbar sein. Darüber hinaus muss sie einen geistigen Inhalt besitzen, also einen Gedanken- oder Gefühlsinhalt aufweisen. Schließlich muss das Werk schöpferische Eigentümlichkeit aufweisen, es muss sich also aus der Masse des Alltäglichen herausheben, wobei die Anforderungen bei der Bewertung dieses Merkmals nicht zu hoch angesetzt werden dürfen.[1]

Um an dieser Stelle konkret zur Zeichentrickmaus zurückzukommen: Zeichnungen werden nach § 2 Abs. 1 Nr. 4 UrhG als Werke der bildenden Kunst geschützt, sofern sie die notwendige Gestaltungshöhe erreichen. Sie fällt demnach unproblematisch unter den Werkbegriff des UrhG.

Mit der Entstehung des Urheberrechts erhält die schaffende Person (also der sog. Urheber) verschiedene Rechte, unter anderem die sog. Urheberpersönlichkeitsrechte. Diese umfassen das Recht zu bestimmen, ob und wie das Werk veröffentlicht wird, das Namensnennungsrecht sowie das Recht, sich gegen Entstellung oder Beeinträchtigung des Werkes zu wehren. Auf diese Rechte kann weder vollständig verzichtet werden noch können diese in Deutschland auf eine andere Person übertragen werden.
Der Urheber kann aber die Verwertungsbedingungen seines Werkes bestimmen, sofern keine Schrankenregelungen eingreifen. In der Praxis erteilen Urheber regelmäßig entsprechende Rechteeinräumungen gegen ein Entgelt, damit Dritte ihre Werke verwenden dürfen.

Doch all diese Rechte gelten nicht ewig. Grundsätzlich erlischt das Urheberrecht in Deutschland 70 Jahre nach dem Tod des

1 Siehe auch Strobel, PowerPoint und das Urheberrecht Teil 1, DFN-Infobrief Recht 8/2019.

Urhebers.[2] Gibt es mehrere Urheber an einem Werk, beginnt die Frist erst nach dem Tod des längstlebenden Miturhebers.[3] Bei anonymen, aber veröffentlichten Werken erlischt das Urheberrecht 70 Jahre nach der Veröffentlichung des Werks.[4] Nach Erlöschen eines Urheberrechts wird das Werk „gemeinfrei", das bedeutet, jedermann kann es frei verwenden.

II. Micky Maus und das amerikanische Urheberrecht

Auch in den USA gibt es ein Urheberrecht an Werken und auch dort läuft dieses nach bestimmten Fristen ab. So gilt ebenfalls, dass das Urheberrecht üblicherweise mindestens 70 Jahre nach dem Tod des Urhebers bestehen bleibt. Allerdings führen in den USA rechtliche Besonderheiten wie die Schaffung des Werkes in einem Angestelltenverhältnis dazu, dass Werke, die vor 1978 veröffentlicht wurden, für 95 Jahre seit der Erstveröffentlichung geschützt werden.[5]

Aus diesen Gründen ist die ursprüngliche Form von Micky Maus aus der Zeichentrickgeschichte „Steamboat Willie" von 1928 nun in ihrem letzten urheberrechtlichen Schutzjahr angelangt. Damit wird die ikonische Maus von Walt Disney und Ub Iwerks [6]mit dem Ablauf von 2023 in den Vereinigten Staaten gemeinfrei werden. Das aber nur in ihrer Version von 1928.

Da sich Micky Maus im Laufe der Zeit verändert hat, unterliegen spätere Versionen der Maus weiterhin dem Schutz der Urheberrechte des Unternehmens Walt Disney. Geänderte Variationen der Figur, z. B. durch das Hinzufügen einer Umrandung seiner Augen oder das Vorhandensein von Handschuhen, sind demnach noch über 2023 hinaus geschützt, je nach Veröffentlichungszeitpunkt der veränderten Figur.

Was bedeutet die Gemeinfreiheit nun für Micky? Ab 2024 kann die Figur von 1928 (und übrigens auch alle anderen in „Steamboat Willie" auftauchenden Figuren, wie z. B. Kater Karlo) von jedermann verwendet werden. Als Beispiel kann der Zeichentrickbär Winnie Puuh dienen. Bei diesem sind die Urheberrechte der Originalgeschichten von 1926 schon seit 2022 in den USA gemeinfrei. Dies nahmen Filmproduzenten u.a. zum Anlass, aus dem Bären in einem Horrorfilm einen Serienkiller zu machen.[7]

III. Das Schutzlandprinzip

Doch wie sieht es nun mit dem urheberrechtlichen Schutz der Maus in Deutschland aus? Diesbezüglich ist die Rechtslage vielschichtig und nicht einfach zu durchdringen. Normalerweise gilt im Urheberrecht das sog. „Schutzlandprinzip". Das bedeutet, dass die Schutzfrist des Landes für ein Werk gilt, in welchem der urheberrechtliche Schutz geltend gemacht wird. Geregelt ist das in § 121 Abs. 4 S. 1 UrhG, welcher auf den Inhalt von Staatsverträgen verweist. Ein solcher Staatsvertrag ist die Revidierte Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (RBÜ), welche sowohl von Deutschland als auch den Vereinigten Staaten unterzeichnet wurde und das Schutzlandprinzip in Art. 5 RBÜ festsetzt. Voraussetzung für die Anwendbarkeit der RBÜ ist, dass zum Zeitpunkt des Inkrafttretens der RBÜ die Schutzdauer im Ursprungsland des Werkes nicht abgelaufen ist.[8]
Auf den Fall Micky Maus angewandt heißt das: Die USA sind der RBÜ wesentlich später als Deutschland am 1. März 1989 beigetreten. Daher trat zwischen Deutschland und den USA die RBÜ erst zu diesem Zeitpunkt in Kraft. Da Micky in den USA im März 1989 noch urheberrechtlichen Schutz genoss, sind die Regelungen der RBÜ daher zunächst anwendbar.
Die Anwendung des Schutzlandprinzips bedeutet nun, dass, auch wenn in den USA die Schutzfrist abgelaufen ist, in Deutschland

2 § 64 UrhG.

3 § 65 Abs. 1 UrhG.

4 66 Abs. 1 S. 1 UrhG.

5 Fun Fact: Diese Regelung beruht auf dem „Copyright Term Extension Act" (CTEA) von 1998 – das Gesetz wird umgangssprachlich aufgrund der Lobbyarbeit von Walt Disney auch „Micky-Maus-Schutzgesetz" genannt, da ohne des CTEA die Urheberrechte an der Kultfigur schon früher abgelaufen wären.

6 Tatsächlich entwickelte Walt Disney Micky Maus nicht allein, der bei Walt Disney angestellte Zeichner Ub Iwerks gilt als Miturheber der Figur.

7 Der Film erschien 2023 unter dem Titel „Winnie the Pooh: Blood and Honey".

8 Art. 18 Abs. 1 RBÜ.

gesondert geprüft werden muss, wann die Frist nach deutschem Recht abläuft. Danach würde die oben beschriebene 70-jährige Frist nach dem Tod des Urhebers gelten und die Regelungen der US-amerikanischen Schutzfristen hätte in Deutschland keine Relevanz.

Das bedeutet nun für die Schutzfristberechnung: Weil Micky Maus von mehreren Urhebern geschaffen wurde, begann die Frist, wie oben schon abstrakt skizziert, erst mit dem Tod des letztverstorbenen Urhebers zu laufe. Da Ub Iwerks erst 1971, also fünf Jahre nach Walt Disneys Tod verstarb, würde die Schutzfrist bis 2041 laufen.
Doch so einfach bleibt es nicht. Denn die RBÜ statuiert neben dem Schutzlandprinzip auch, dass die Schutzdauer eines ausländischen Werkes nicht länger andauern kann, als es im Ursprungsland Schutz genießt. Vereinfacht gesagt, wenn der sog. „Schutzfristenvergleich" ergibt, dass im Ursprungland des Werkes der urheberrechtliche Schutz abgelaufen ist, kann das deutsche Urheberrecht diesen Schutz nicht mit einer längeren Frist erhalten. In diesem Fall ist das Werk dann auch in Deutschland als gemeinfrei anzusehen.

Die Anwendung des Schutzfristenvergleichs würde daher nun dazu führen, dass trotz der längeren deutschen Schutzfrist die Gemeinfreiheit in den USA ab dem kommenden Jahr auch in Deutschland gelten würde. Der Ur-Micky von 1928 würde demnach auch hier seinen urheberrechtlichen Schutz verlieren.
Doch wer nun dachte, dass die Fristbestimmung des Schutzes damit erledigt sei, liegt leider falsch. Denn es gibt noch einen weiteren relevanten Staatsvertrag: das Übereinkommen zwischen dem Deutschen Reich und den Vereinigten Staaten von Amerika über den gegenseitigen Schutz der Urheberrechte von 1892. Trotz seines Alters ist dieses Abkommen nach wie vor in Kraft und entfaltet damit Rechtswirkung. Auch die RBÜ regelt, dass das Abkommen Vorrang gegenüber den Regelungen der RBÜ genießt und anwendbar bleibt.[9]
Dieses deutsch-amerikanische Abkommen legt fest, dass die Werke US-amerikanischer Urheber in Deutschland wie inländische Werke behandelt werden. Somit findet das Schutzlandprinzip zwischen den USA und Deutschland nun über diesen juristischen Umweg quasi doch wieder Anwendung. Und damit kommen in Deutschland trotz der Beschränkungen der RBÜ wieder allein die deutschen Schutzfristen auch für US-amerikanische Werke zur Anwendung. Dadurch, dass das Abkommen (anders als die RBÜ) keinen Schutzfristenvergleich vorsieht, bleibt es bei der reinen Anwendung der deutschen Schutzfrist. Das Ablaufen der US-amerikanischen Frist spielt daher keine Rolle. In der Konsequenz wird der urheberrechtliche Schutz von Micky Maus in Deutschland daher wohl weiter bestehen bleiben und zumindest hierzulande noch nicht gemeinfrei werden.

Übrigens: Dass die Bestimmung von Schutzfristen innerhalb der verschiedenen Länder nicht einfach ist, zeigen auch unterschiedliche gerichtliche Verfahren. So musste zum Beispiel der Bundesgerichtshof (BGH) in einer Entscheidung über die Tarzan-Romane[10] nicht nur das deutsch-amerikanische Abkommen von 1892 und die RBÜ prüfen, sondern es kam darüber hinaus zur Prüfung des Welturheberrechtsabkommens (WUA), des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) und des Urheberrechtsvertrags der Weltorganisation für geistiges Eigentum (WCT), um die Schutzfristen der Romane bestimmen zu können. Trotz dieser umfangreichen Prüfung übt die juristische Literatur auch an diesem Urteil Kritik, insbesondere dass die europäischen Richtlinien nicht ausreichend beachtet worden seien.

IV. Markenschutz

Zurück zu unserer vier-Finger-Maus: Ob Micky nach dem Ablaufen des Urheberrechts in den USA auch eine Zukunft als Serienkiller bevorsteht, bleibt abzuwarten. Zumindest in Deutschland scheint die Maus noch einige Schutzjahre des Urheberrechts genießen zu dürfen.
Doch auch ohne Urheberrechte wird Walt Disney ihre ikonische Figur sicherlich nicht ohne Weiteres aufgeben. Denn auch wenn das Urheberrecht an der Ursprungsfigur erlischt, hält Disney wohl weiterhin Markenrechte an Micky Maus.

Eine Marke ist ein rechtlich geschütztes Zeichen, das meist Waren oder Dienstleistungen kennzeichnet.[11] So ist zum Beispiel das geschwungene McDonald's M wohl eine der bekanntesten Marken weltweit. Markenrechte schützen den Markeninhaber vor der unbefugten Nutzung seiner Marke zu kommerziellen

9 Art. 20 RBÜ.

10 Bundesgerichtshof, Urt. v. 26.2.2014 – I ZR 49/13, Tarzan.

11 Zum Markenrecht im Allgemeinen: Uphues, Du bist mir ja ‚ne Marke!, DFN-Infobrief Recht 8/2019.

Zwecken. Aber anders als Urheberrechte laufen Markenrechte nicht nach einem bestimmten Zeitraum aus, sondern bleiben bestehen, solange die Marke genutzt wird.
Dadurch, dass die Steamboat-Willie-Version der Maus immer wieder in und auf Produkten von Walt Disney aufgetaucht ist, ist davon auszugehen, dass die Figur von den Markenrechten von Disney umfasst ist. Diese Markenrechte an der Originalfigur von Micky Maus ermöglichen Walt Disney daher auch über die urheberrechtlichen Fristen hinaus Schutz vor zumindest der unerlaubten wirtschaftlichen Nutzung der Figur.

Bei einer Kultfigur wie Micky Maus wird es also auch unabhängig vom Urheberrecht noch lange dauern, bis Disney die wirtschaftliche Nutzung faktisch einstellt. Das bedeutet, solange die Marke besteht, kann Disney z. B. bestimmen, wer den Ur-Micky auf eine Tasse drucken und verkaufen darf. Für eine solche Nutzung kann weiterhin Walt Disney die entsprechenden Rechte einräumen und unerlaubte Nutzungen untersagen.

V. Fazit

Schon allein der Umstand, dass dieser Beitrag eigentlich als Kurzbeitrag angedacht war und durch die Recherche über das Bestehen des Urheberrechts an Micky Maus in seinem Inhalt doch zu einem umfangreichen Beitrag des DFN-Infobriefs Recht angewachsen ist, zeigt, wie komplex das internationale Urheberrecht werden kann. Die vielen Änderungen der urheberrechtlichen Vorgaben sowohl in Deutschland als auch den USA sowie der internationalen Abkommen sorgen in der Praxis schnell für Verwirrung und Unsicherheit. Das zeigen auch die Urteile der höchsten Gerichte sowie die Diskussionen in der juristischen Literatur anschaulich. Insoweit ist es gut möglich, dass die Schutzfrist für den 1928er Micky in Deutschland von anderen Ansichten anders bewertet wird.

Soweit jedenfalls die Gemeinfreiheit für ein Werk festgestellt werden kann, bedeutet dies, dass das Werk aus urheberrechtlicher Sicht von jedermann auch kommerziell frei benutzt werden kann. So kann die Verbreitung oder Bearbeitung ohne Erteilung von Nutzungsrechten vorgenommen werden. Hierdurch können dann wieder neue Werke entstehen, welche ein Urheberrecht begründen, wenn sie die oben dargestellten Voraussetzungen erfüllen. Das für die Bearbeitung benutzte gemeinfreie Werke bleibt dennoch gemeinfrei für alle nutzbar.

Doch müssen vor der freien Nutzung eines Werks, wie aufgezeigt, stets andere gewerbliche Schutzrechte wie z. B. das Markenrecht beachtet werden. Insoweit kann auch die Nutzung von urheberrechtlich gemeinfreien Werken durch andere Rechte weiterhin eingeschränkt sein. Wie weit die Einschränkungen gehen, ist individuell zu prüfen.
Doch für die Wissenschaft und Forschung ist die Gemeinfreiheit eines Werkes stets ein Gewinn. Denn die Nutzung eines gemeinfreien Werkes in z. B. Folien für eine Vorlesung[12] oder anderen Lehrunterlagen[13] stellt keine kommerzielle Nutzung dar. Insoweit wird die Nutzung gemeinfreier Werke zu universitären Zwecken regelmäßig unabhängig von kommerziellen Schutzrechten zulässig sein.[14]

12 Zur Nutzung von fremden Werken in Folien im Allgemeinen: Strobel, PowerPoint und das Urheberrecht Teil 1, DFN-Infobrief Recht 8/2019; Strobel, PowerPoint und das Urheberrecht Teil 2, DFN-Infobrief Recht 9/2019.

13 Zum Urheberrecht im Distance Learning: Wellmann, Social Distance Learning, DFN-Infobrief Recht Sonderausgabe Covid-19/2020.

14 Uphues, Du bist mir ja ‚ne Marke!, DFN-Infobrief Recht 8/2019.

Kurzbeitrag: Nicht (un)erheblich!

Das Urteil des EuGH zum immateriellen Schadensersatz nach der DSGVO

von Johanna Voget

Der Europäische Gerichtshof (EuGH) hat zu den viel diskutierten Fragen um den immateriellen Schadensersatzanspruch nach der Datenschutzgrundverordnung (DSGVO) Recht gesprochen und damit endlich alles geklärt - oder etwa doch nicht? Zu dem Ausgangsverfahren und der Argumentation des Generalanwalts Sánchez-Bordona berichtete der DFN-Infobrief Recht bereits ausführlich.[1]

I. Hintergründe und Verfahren

Ein kurzer Reminder zum Einstieg: Art. 82 Abs. 1 DSGVO statuiert, 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.

Mit den Voraussetzungen und dem Umfang des datenschutzrechtlichen Schadensersatzanspruchs hat sich die Forschungsstelle Recht in der Vergangenheit bereits wiederholt intensiv beschäftigt.[2]

Dem EuGH lag nun ein Vorabentscheidungsersuchen aus Österreich zur Auslegung der Regelung des Art. 82 DSGVO vor. Gegenstand des zugrundeliegenden Verfahrens vor den österreichischen Gerichten war das Verhalten der Post AG, die mit Hilfe eines Algorithmus und sozialdemografischer Merkmale versucht hatte, die Parteipräferenz von Personen zu ermitteln. Der Kläger berief sich darauf, in diese Datenverarbeitung nicht eingewilligt zu haben und eine große Verärgerung sowie ein Gefühl der Bloßstellung durch seine angebliche Affinität zu einer Partei verspürt zu haben. Er verlangte daher 1.000 Euro Schadensersatz von der Beklagten, der Österreichischen Post.[3] Der oberste Gerichtshof zweifelte an der Begründetheit dieses Begehrens, und legte dem EuGH die Fragen vor, ob der bloße Verstoß gegen die DSGVO ausreiche, um einen Schadenersatzanspruch zu begründen und ob für den Ersatz des entstandenen immateriellen Schadens eine bestimmte Erheblichkeit vorliegen müsse.

Der Generalanwalt Sánchez-Bordona vertrat in seinen Schlussanträgen vom 06. Oktober 2022 eine sehr restriktive Auslegung, nach welcher der Schadensersatz stets das Vorliegen eines nachweisbaren Schadens voraussetze, denn andernfalls handele es sich vielmehr um eine Sanktion oder einen Strafschadensersatz.[4] Hierbei sei dann auch nicht jeder entstandene Nachteil als ersatzfähiger immaterieller Schaden anzusehen – im Ergebnis sei also wohl eine gewisse Erheblichkeit zu fordern.

II. Was sagt der EuGH dazu?

Nun liegt die Entscheidung aus Luxemburg vor (Urt. v. 4.5.2023, Az.: C-300/21), die in ihrer Kernaussage lautet: Nicht jeder Verstoß gegen die DSGVO reicht automatisch für einen Anspruch auf

1 Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

2 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.

3 Zum Sachverhalt: Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

4 Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

immateriellen Schadensersatz aus - einer Erheblichkeitsschwelle bedarf es jedoch nicht.[5]

Ganz grundsätzlich sei für den Schadensersatzanspruch nach Art. 82 DSGVO das Vorliegen dreier kumulativer Voraussetzungen erforderlich: Es müsse ein Verstoß gegen die DSGVO, ein materieller oder immaterieller Schaden und ein ursächlicher Zusammenhang zwischen Schaden und Verstoß vorliegen.
Hinsichtlich der Frage nach dem Erfordernis einer gewissen Erheblichkeit im Rahmen immaterieller Schäden weichen die Richter dann aber von der Argumentation des Generalanwalts ab. Die DSGVO kenne keine Erheblichkeitsschwelle. Vielmehr stelle der Erwägungsgrund 146 zur DSGVO klar, dass der Begriff des Schadens weit auf eine Art und Weise ausgelegt werden soll, die den Zielen dieser Verordnung in vollem Umfang entspreche. Die betroffenen Personen sollen danach einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Daher stünde das Erfordernis einer gewissen Erheblichkeit im Widerspruch zum unionsrechtlich weiten Verständnis des Schadensbegriffs.
Die Festlegung der Kriterien für die Ermittlung des Schadensumfangs habe dann wiederum nach dem Recht der einzelnen Mitgliedstaaten selbst zu erfolgen.

Der Betroffene muss also darlegen, dass er einen Schaden hat. Hierbei darf die Erheblichkeit des Schadens zwar kein anspruchsausschließender Umstand sein. Auf der anderen Seite sind aber konkrete Ausführungen zu einem Schaden notwendig. An diese sind dann jedoch auch keine hohen Anforderungen zu stellen, um das Ziel der DSGVO, den Betroffenen einen vollständigen und wirksamen Schadensersatz zu verschaffen, nicht zu gefährden.

III. Und was bedeutet das jetzt?

Erheblich muss der immaterielle Schaden also nicht sein. So ganz unerheblich darf er dann wiederum aber auch nicht sein. Ob denn nun „Ärger“ oder „Unsicherheit“ grundsätzlich ausreichen, um einen Schaden zu begründen und wenn ja, wie konkret dies sodann dargelegt werden muss, bleibt weiterhin nicht hinreichend geklärt Erforderlich ist daher nun eine Ausgestaltung und Weiterentwicklung der Entscheidung durch die Gerichte der Mitgliedstaaten.

Die Bedeutung des (immateriellen) Schadensersatzes wird also zukünftig davon abhängen, welche Anforderungen die nationalen Gerichte nach eigenem Ermessen an den Darlegungsaufwand stellen.
Wie sich die aktuelle Entscheidung in der Praxis auswirken wird und ob sie einen Gewinn bedeutet, bleibt damit vorerst abzuwarten.

5 https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=3975196 , [Stand vom 08.05.2023].

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