infobrief recht DFN

3 / 2022
März 2022

Suche Schriftart: Jung, dynamisch, datenschützend

Das Landgericht München I urteilt, dass die Einbindung von Google Fonts ohne Einwilligung der betroffenen Person rechtswidrig ist

Nicht nur das Kind braucht einen Namen

Eine Entscheidungsbesprechung zur Klarnamenpflicht in sozialen Netzwerken

Handy weg? EncroChat!

Eine juristische Aufarbeitung des Hacks der verschlüsselten Kommunikationsplattform „EncroChat“

Suche Schriftart: Jung, dynamisch, datenschützend

Das Landgericht München I urteilt, dass die Einbindung von Google Fonts ohne Einwilligung der betroffenen Person rechtswidrig ist

von Nicolas John

Webseitenbetreibenden steht für ihre Webseitengestaltung eine unüberschaubare Menge an Tools, Diensten und Plug-Ins zur Verfügung. Oft ist die Implementierung dieser Dienste durch Baukastensysteme praktisch, denn es geht insbesondere für kleine Einrichtungen oder Laien schnell und einfach. Das Augenmerk muss aber neben einer ansprechenden Funktionalität der Webseite auch auf dem Datenschutz liegen, wenn personenbezogene Daten verarbeitet werden. Doch kann die Gefahr oft in kleinen Details liegen. So hatte eine Webseitenbetreiberin die auf der Seite verwendete Schriftart von einem Google-Dienst eingebunden. Hierdurch wurden die IP-Adressen der Seitenbesuchenden an Google-Server übermittelt. Doch die Betreibende hatte die nach Ansicht des Landgerichts (LG) München I (Urteil vom 20. Januar 2022, Az. 3 O 17493/20) hierfür erforderliche Einwilligung des betroffenen Klägers nicht eingeholt und verurteilte die Betreiberin letztendlich zur Zahlung eines Schadensersatzes.

I. Hintergrund

1. Google Fonts

Google Fonts ist ein Online-Dienst, welcher es Webseitenbetreibenden ermöglicht, verschiedene Schriftarten kostenlos auf der eigenen Webseite zu implementieren. Es gibt unterschiedliche Wege, die angebotenen Schriftarten auf der Webseite einzubinden. Bei einer statischen Einbindung lädt der Betreibende die Schriftart zunächst herunter. Diese Daten werden anschließend auf den Webseiten-Server hochgeladen, um sie dann in der Webseite einzubinden.

Alternativ lässt sich die Schriftart auch dynamisch einbinden. Das bedeutet, dass der Webseitenbetreibende die Schriftart nicht zuerst herunterladen muss, sondern die Schriftart direkt von den Servern von Google in seine Webseite einbindet.
Der Unterschied zwischen den beiden Methoden ist für den Besuchenden der Webseite nicht ohne weiteres sichtbar. Bei der statischen Variante wird bei dem Besuch der Seite keine Verbindung zu Googles Servern aufgebaut, da die Schriftart auf dem eigenen Webseiten-Server gespeichert ist. Dagegen ist bei der dynamischen Einbindung der Abruf der Schriftart von den Servern von Google erforderlich und geschieht jedes Mal, wenn ein Besuchender auf die Webseite zugreift. Im Zuge dieser Abfrage wird die IP-Adresse des besuchenden an Google übermittelt.

2. Internetprotokoll-Adressen und Datenschutz

IP-Adressen werden Geräten im Internet zugewiesen und ermöglichen auf diese Weise das Gerät im Netzwerk wiederzuerkennen. Sie sind vergleichbar mit einer Postadresse oder einer Telefonnummer im realen Leben: durch die Adresse oder Nummer ist das Haus oder das mit der Telefonnummer verbundene Telefon erreichbar und wiedererkennbar. Konkret bedeutet

das: wenn ein digitales Datenpaket an ein bestimmtes Gerät im Internet geschickt werden soll, dann können die Router als Übertragungseinheiten das richtige Gerät im Internet anhand der IP-Adresse finden. Wenn der Nutzende eine Internetadresse aufruft, wird durch einen Namensserver abgefragt, welche IP-Adresse mit der angefragten Domain aktuell verknüpft ist. Einige Server oder Webseiten haben fest zugewiesene, sogenannte statische IP-Adressen, damit die Webseite oder der Dienst immer unter der gleichen Adresse erreichbar ist. Doch da die Adressen nach dem Internetprotokoll endlich sind und es mehr Geräte als IP-Adressen im Netz gibt, werden die IP-Adressen regelmäßig neu vergeben. Dies geschieht, wenn sich ein Gerät neu in das Internet einwählt, zum Beispiel der Router zu Hause nach einem Neustart. Diese wechselnden IP-Adressen werden dynamische IP-Adressen genannt.

In der rechtlichen Betrachtung haben diese dynamischen IP-Adressen in der Vergangenheit vermehrt für Diskussionen gesorgt. Denn durch das Wechseln der Adresse ist es nicht ohne weiteres möglich, die Person hinter der IP-Adresse zu ermitteln. Daher war fraglich, ob IP-Adressen überhaupt personenbezogene Daten darstellen. Nachdem sich sowohl der Bundesgerichtshof (BGH)[1] als auch der Europäische Gerichtshof (EuGH)[2] mit dieser Frage beschäftigten, steht fest, dass sie rechtlich als personenbezogene Daten einzuordnen sind. Ist die Identität der betroffenen Person nämlich für den Betreibenden einer Webseite mithilfe Dritter, nämlich unter Einschaltung der zuständigen (Ermittlungs-)Behörde und des Internetzugangsanbieters, anhand der IP-Adresse zu ermitteln, lässt sich, wie im Rahmen der statischen IP-Adresse, ein Personenbezug problemlos herstellen. An diese Rechtsprechung knüpft der nachfolgende Fall an.

II. Sachverhalt

Der Sachverhalt der Entscheidung ist überschaubar: Die Beklagte hatte die dynamische Möglichkeit der Einbindung von Google Fonts genutzt und eine nicht auf ihren Servern gespeicherte Schriftart in die Webseite eingebunden. Auf die damit verbundene Übermittlung der IP-Adresse der Besuchenden an Google hatte die Beklagte nicht hingewiesen und keine Einwilligung des Klägers eingeholt. Aus diesem Grund rief der Kläger das Gericht an und verlangte die Unterlassung der Übermittlung sowie Schadensersatz.

III. Entscheidung

In seiner Entscheidung gab das LG München I dem Kläger Recht und folgte damit der gängigen Rechtsprechung des BGH. Bereits zu Beginn des Urteils wurde dabei festgestellt, dass die dynamische IP-Adresse des Klägers für den Webseitenbetreibenden ein personenbezogenes Datum darstelle, da der Betreibende wie oben beschrieben abstrakt über die Möglichkeit verfüge, die betroffene Person anhand der IP-Adresse zu bestimmen. Ausreichend sei, dass die Möglichkeit der Ermittlung abstrakt bestehe. Nicht erforderlich sei hingegen, dass die Beklagte oder Google eine konkrete Möglichkeit zur Ermittlung haben.

Aufgrund dieser Einordnung sei eine Datenverarbeitung der IP-Adresse durch einen Erlaubnistatbestand der Datenschutz-Grundverordnung (DSGVO) zu rechtfertigen. Bei der Verwendung von Google Fonts muss für die Weiterleitung der IP-Adresse an Google folglich ein Rechtfertigungsgrund vorliegen. Die Beklagte war der Ansicht, dass dies wegen eines berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f) DSGVO der Fall sei. Diese Norm erlaubt eine Datenverarbeitung, wenn die verantwortliche Person ein überwiegendes Interesse an der Verarbeitung gegenüber den schutzwürdigen Interessen der betroffenen Person hat. Dieses überwiegende Interesse muss im Rahmen einer Abwägung der widerstreitenden Interessen festgestellt werden. Von Relevanz ist daher im vorliegenden Fall die Möglichkeit einer statischen Einbindung der Schriftart. Hierdurch kann der Verantwortliche ohne großen Aufwand die Webseite in ihrer Form auch ohne eine Übertragung der IP-Adresse an Google einrichten.

Aus diesem Grund stellte das LG München I fest, dass das behauptete berechtigte Interesse nicht vorliegen könne, da die Nutzung von Google Fonts durch vorheriges Herunterladen und Hochladen in den eigenen Webspace auch ohne die Weiterleitung der IP-Adresse möglich sei. Eine Datenverarbeitung würde so gerade nicht stattfinden. Da die Beklagte zuvor keine Einwilligung des Klägers für die Weiterleitung der IP-Adresse an Google eingeholt hatte, fehle es hier an einem

1 BGH, Urt. v. 16.05.2017, Az. VI ZR 135/13; im Detail hierzu: Mörike, BGH bestätigt: IP-Adressen sind personenbezogene Daten, DFN-Infobrief Recht 9/2017.

2 EuGH, Urt. v. 19.10.2016, Az. C-582/14; hierzu im Detail: Sydow, Speichern ist relativ?, DFN-Infobrief Recht 12/2016.

Rechtfertigungsgrund für die Verarbeitung des personenbezogenen Datums. Die Rechtswidrigkeit war folglich zu bejahen.

Interessant ist der weitere Vortrag der Beklagten: Sie vertrat die Ansicht, dass es die Pflicht des Klägers sei, seine eigene IP-Adresse zu „verschlüsseln". Gemeint ist an dieser Stelle vermutliche die Verschleierung bzw. Unterdrückung der IP-Adresse, wie dies beispielsweise durch die Nutzung eines Virtual Private Networks (VPN) möglich ist. Das Bestehen einer solchen Pflicht verneint das LG München I jedoch, da dies dem Zweck des Datenschutzrechts zuwiderlaufe. Dieses solle die natürliche Person bei der Verarbeitung ihrer personenbezogenen Daten gerade vor einer Beeinträchtigung ihrer Rechte schützen. Wenn hingegen betroffene Personen Maßnahmen ergreifen müssten um eine Rechtsverletzung zu vermeiden, würde eine solche Verpflichtung zur Verschleierung diesen Zweck dagegen umkehren. Die Verantwortlichen würden sich folglich ihrer datenschutzrechtlichen Verpflichtungen entziehen können und der Datenschutz würde leerlaufen. Insoweit schließt sich das Landgericht dem Urteil des LG Dresden vom 11. Januar 2019 (Az. 1a O 1582/18) an. Schon in diesem Urteil stellte das LG Dresden fest, dass es dem Besuchenden einer Webseite nicht zuzumuten sei, die eigene IP-Adresse zu verschleiern.[3]

Einen weiteren interessanten Aspekt bietet das Urteil des LG München I am Ende bezüglich des Schadensersatzanspruchs, denn das Landgericht verurteilt die Beklagte zur Zahlung eines Schadensersatzes in Höhe von 100 Euro. Als Begründung führt es an, dass es durch die Übermittlung der IP-Adresse zum „Kontrollverlust" des Klägers über sein personenbezogenes Datum gekommen sei und das damit vom Kläger verbundene „Unwohlsein so erheblich" sei, dass der Schadensersatzanspruch gerechtfertigt sei. Mit der Übermittlung an Google in die USA sei außerdem zu berücksichtigen, dass dort kein angemessenes Datenschutzniveau gewährleistet sei und der Anspruch auf Schadensersatz präventiv den Anreiz schaffen solle, entsprechende Sicherungsmaßnahmen zu schaffen.

Mit Blick auf einen Beschluss des Bundesverfassungsgerichts (BVerfG) vom 14. Januar 2021 (Az. 1 BvR 2853/19) ist die Entscheidung bezüglich des Schadensersatzanspruchs bemerkenswert: Nach diesem Beschluss des BVerfG ist eine Klage dem EuGH vorzulegen, in welcher der Umfang eines Schadensersatzes bzw. Schmerzensgeldes zu klären sei. Die Rechtslage sei vom EuGH weder erschöpfend geklärt worden, noch lägen die notwendigen Voraussetzungen vor, dass der Umfang unmittelbar aus der DSGVO bestimmt werden könne. Entgegen der Auffassung des BVerfG sah sich das LG München I in dem vorliegenden Verfahren offenbar nicht in der Vorlagepflicht und wartete auch nicht etwaige anhängige Verfahren ab.

IV. Fazit und Auswirkungen für Hochschulen und Forschungseinrichtungen

Das Urteil ist zunächst inhaltlich keine Überraschung. Es führt die bisher geltende Rechtsprechung zum Datenschutz bei IP-Adressen konsequent fort und zeigt lediglich exemplarisch an Google Fonts, worauf Webseiten-Betreibende bei der Einbindung von externen, dynamischen Diensten auf ihrer Webseite zu achten haben. Das Urteil lässt aber auch erkennen, dass die Einbindung eines dynamischen Dienstes datenschutzrechtlich nicht gänzlich verboten ist. Eine Verwendung kann möglich sein, wenn die erforderliche Einwilligung von der betroffenen Person durch ein entsprechendes Banner eingeholt wird.

Dennoch kann das Landgericht nicht über die Frage entscheiden, ob US-Dienste im Lichte des „Schrems II"-Urteils des EuGHs[4] tatsächlich rechtskonform mit einem Einwilligungsbanner verwendet werden können. Insbesondere die Einbeziehung der aktuellen Standarddatenschutzklauseln (SCC) der Europäischen Kommission[5] sowie der Umfang vorzunehmender technischer und organisatorischer Maßnahmen (TOMs)[6] ist bislang ungeklärt. Es ist daher weiterhin nicht sicher, ob die Verwendung der SCC für Datenexporte die USA einer gerichtlichen Überprüfung standhalten.

Spannend stellt sich aber die Zusprechung des Schadensersatzes dar. Zwar mögen 100 Euro aus dem vorliegenden Urteil der Höhe nach zunächst nicht nach viel klingen, doch öffnet sich

3 Hierzu im Detail: Baur, Unmaskiert wird abkassiert, DFN-Infobrief Recht 8/2019.

4 Im Detail dazu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

5 Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

6 Exemplarisch bei der Verwendung von Videokonferenzsoftware: John, Corona is calling, DFN-Infobrief Recht Sonderausgabe Covid-19/2020; anhand der Verwendung von Microsoft 365: John, New Schrems, new Me(crosoft), DFN-Infobrief 2/2022.

das Tor für Abmahnung und Schadensersatzforderungen weit, sollte sich die Auffassung des LG München I in der Rechtsprechung durchsetzen. Darüber hinaus handelte es sich in dem vorliegenden Verfahren nur um eine Person. Die Summen des zu zahlenden Schadensersatzes erreichen andere Dimensionen, wenn eine Webseite mehrere tausend Besuchende hat. Diese wären bereits durch den Besuch der Webseite klagebefugt.

Für Hochschulen und Forschungseinrichtungen ist das Urteil daher auch von großer Relevanz, denn nahezu jede Einrichtung hält eine eigene Webpräsenz vor. Es sind insbesondere die Verantwortlichen für die Webseiten angehalten, ihre Plug-Ins und eingebundenen Dienste zu überprüfen, ob eine Übertragung von personenbezogenen Daten (wie der IP-Adresse) an Dritte stattfindet. In einem weiteren Schritt sollte durch ein entsprechendes Banner über die Verwendung der Dienste informiert werden und die Einwilligung des Webseiten-Besuchenden eingeholt werden. Falls es sich um Dienste aus Nicht-EU-Staaten handelt, muss darüber hinaus geprüft werden, ob der Datenexport durch einen Angemessenheitsbeschluss oder vereinbarten SCCs gerechtfertigt ist.

Nicht nur das Kind braucht einen Namen

Eine Entscheidungsbesprechung zur Klarnamenpflicht in sozialen Netzwerken

von Owen Mc Grath

Seit längerer Zeit schon wird über die Klarnamenpflicht in sozialen Netzwerken diskutiert. Urteile der letzten Jahre haben die Materie scheinbar geordnet. Nun wirft der Bundesgerichtshof (BGH) diese vermeintliche Klarheit mit einem aktuellen Urteil über den Haufen und verdeutlicht die verworrene Gesetzeslage zu der einschlägigen Materie.

I. Klarnamenpflicht

Eine Klarnamenpflicht bezeichnet die Verpflichtung zur Verwendung des tatsächlichen Namens bei der Nutzung eines sozialen Netzwerkes. Dies soll dazu dienen, Straftaten und Hassnachrichten im Netz vorzubeugen und für den Fall, dass diese doch begangen werden, eine Verfolgung zu erleichtern.
Durch die Verwendung des bürgerlichen Namens und dem damit einhergehenden Mangel an Anonymität sind Nutzer sozialer Netzwerke weniger dazu geneigt, sich in beleidigender oder sogar strafrechtlich relevanter Weise zu äußern.

Begeht jemand in einem sozialen Netzwerk aber dennoch eine Straftat oder Ordnungswidrigkeit, ist eine Verfolgung dieser Person – für den Fall, dass sie unter einem Nickname oder Pseudonym handelte – nur schwer möglich. Meist bieten solche Namen keine Anhaltspunkte über den Wohnort oder den Verbleib der straffälligen Person. Die Verpflichtung zur Verwendung eines Klarnamens ermöglicht der Ermittlungsbehörde zumindest den Täterkreis einzugrenzen und gezielte Ermittlungen einzuleiten.

Insbesondere im Lichte des Datenschutzes und der grundgesetzlich verankerten informationellen Selbstbestimmung (Ausprägung des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz) stellt sich die Frage, ob Nutzer gezwungen werden können, einen Klarnamen zu verwenden.
In den letzten Jahren wurde sich durchaus kontrovers zu der Pflicht der Verwendung eines Klarnamens in Rechtsprechung und Schrifttum geäußert. Argumentativ stehen Datenschutz und informationelle Selbstbestimmung der Nutzer auf der einen Seite und Verhinderung von Hass und Hetze sowie Straftaten im Netz auf der anderen Seite.
Wie diese Diskussion an konkrete Normen anzuknüpfen ist und welchen Stand die Rechtsprechung zuletzt einnahm, zeigen die folgenden Ausführungen.

II. Aktuelles Urteil des BGH

Ende Januar dieses Jahres entschied der BGH in zwei Verfahren zur Pflicht der Verwendung von Klarnamen.[1] In beiden Fällen ging es um das gleiche Netzwerk, welches in seinen Allgemeinen Geschäftsbedingungen (AGB) eine Verwendung von Klarnamen vorschreibt. Die Kläger verwendeten auch nach Aufforderung des Netzwerkes keine Klarnamen. Daraufhin wurden ihre Benutzerkonten gesperrt.

Einer der Kläger kam daraufhin der Forderung des Netzwerkes nach und änderte seinen Nutzernamen in den Klarnamen. Er klagte nun darauf, dass das Netzwerk es unterlassen soll, eine Änderung dieses Klarnamens in ein Pseudonym zu verhindern. Der andere Kläger verwendete weiterhin keinen Klarnamen und forderte in der Klage die Unterlassung der Sperrung seines Nutzerkontos.

Bisher liegt zu den Entscheidungen leider nur eine Pressemitteilung und keine Volltextveröffentlichung vor. Die Begründungen des BGH sind daher bislang nur grob skizziert.
Im deutschen Recht unterliegen AGB einer Inhaltskontrolle (§ 307 Bürgerliches Gesetzbuch [BGB]). Durch diese kann die

1 BGH, Urteile vom 28.01.2022, Az.: III ZR 3/21 und 4/21.

Unwirksamkeit einzelner Bestimmungen festgestellt werden. AGB sind insbesondere dann unwirksam, wenn sie unvereinbar mit dem wesentlichen Grundgedanken einer gesetzlichen Regelung sind (§ 307 Abs. 2 Nr.1 BGB).
Im vorliegenden Fall sah der BGH die Vorgabe, dass die Nutzer einen Klarnamen verwenden müssen, als unvereinbar mit § 13 Abs. 6 S. 1 Telemediengesetz alte Fassung (TMG a.F.) an. Diese Norm schreibt vor, dass ein Diensteanbieter die Nutzung der Telemedien anonym oder unter Pseudonym zu ermöglichen hat, „soweit dies technisch möglich und zumutbar ist". Laut BGH ist zwar eine Angabe des Klarnamens im Innenverhältnis, also zwischen Nutzer und Netzwerk, erforderlich. Im Außenverhältnis zu anderen Nutzern sei jedoch eine Pseudonymisierung zu ermöglichen.

III. Entscheidung der Vorinstanz

In einer der Vorinstanzen entschied das OLG München, dass eine Klarnamenpflicht bei der Nutzung sozialer Netzwerke mit § 13 Abs. 6 S. 1 TMG a.F. vereinbar sei.[2] Argumentiert wurde insofern nicht mit der eigentlichen Wirkung der Vorschrift, sondern mit der Systematik des Gesetzes. So sei das Telemediengesetz im Lichte der Datenschutz-Grundverordnung (DSGVO) zu sehen. Die DSGVO genießt als EU-Recht Anwendungsvorrang vor nationalem Recht. Widerspricht das nationale Recht (hier: TMG) dem EU-Recht (hier: DSGVO), ist das nationale Recht unanwendbar.

Im Gegensatz zum TMG äußert sich die DSGVO nicht explizit zur anonymisierten oder pseudonymisierten Nutzung von Netzwerken. Nach Einschätzung des OLG München sei diese Nutzung allerdings bewusst nicht geregelt. Argumentiert wird, dass ein Recht auf pseudonyme Nutzung im Gesetzgebungsprozess zwar angesprochen, aber bewusst nicht geregelt wurde. Man spricht von einem „beredten Schweigen". Der europäische Gesetzgeber wolle nicht vorschreiben, dass eine Nutzung von sozialen Netzwerken unter einem anderen als dem Klarnamen möglich sei. Der § 13 Abs. 6 S. 1 TMG a.F. sei in unionsrechtskonformer Auslegung so zu interpretieren, dass sich der Widerspruch zum EU-Recht auflöst. Dies tut das OLG über das Merkmal der Zumutbarkeit, welche die Norm zur Voraussetzung der Ermöglichung der Pseudonymisierung macht. Um die Zumutbarkeit festzustellen oder abzulehnen, seien im Rahmen einer Verhältnismäßigkeitsprüfung die Interessen der Plattformbetreiber und der Nutzer, die ein Pseudonym verwenden wollen, zum Ausgleich zu bringen. Das OLG München sieht die Interessen an der Verhinderung von Cyber-Mobbing und Hetze im Netz als so überwiegend an, dass eine Ermöglichung der pseudonymen Nutzung nicht zumutbar ist.
Mithin ist der Einschätzung des OLG folgend § 13 Abs. 6 S. 1 TMG a.F. in unionsrechtskonformer Auslegung nicht zu entnehmen, dass dieser eine Klarnamenpflicht verbietet. Dementsprechend seien die AGB des beklagten Netzwerks auch nicht mit dem Grundgedanken des § 13 Abs. 6 S. 1 TMG a.F. unvereinbar und es liege keine Unwirksamkeit nach § 307 Abs. 2 Nr.1 BGB vor.

IV. Korrektur durch den BGH

Nach dem Dargelegten drängt sich die Frage auf, warum der BGH den § 13 Abs. 6 S. 1 TMG a.F. nicht auch, wie das OLG, im Lichte der DSGVO gesehen hat und zum Ergebnis kam, dass eine Klarnamenpflicht durchaus angebracht sei und die AGB entsprechend zulässig seien.
Das Ergebnis des OLG München ist allerdings nicht so differenziert und zutreffend, wie es auf den ersten Blick scheint. Während das OLG schlichtweg die DSGVO anwendete, stellte der BGH auf den Zeitpunkt der Einbeziehung der in Frage stehenden AGB in den Vertrag ab. Zu diesem Zeitpunkt galt nicht die DSGVO, welche erst ab 25. Mai 2018 anzuwenden war, sondern deren Vorgänger, die Datenschutzrichtlinie von 1995 (DS-RL). Dementsprechend sei für die Wirksamkeit der AGB die DS-RL und nicht die DSGVO anzuwenden.

Genau wie das OLG führt auch der BGH im Rahmen der Prüfung der Zumutbarkeit der Pseudonymisierung des § 13 Abs. 6 S. 1 TMG a.F. eine Interessenabwägung durch. Diese Abwägung scheint der BGH allerdings, soweit aus der Pressemitteilung ersichtlich, nicht durch die nach seiner Einschätzung geltende europäische Datenschutzrichtlinie zugunsten der Betreiber sozialer Netzwerke beeinflusst zu sehen. Vielmehr sieht er den Art. 6 Abs. 1 lit. c DS -RL, welcher sich in vergleichbarer Form auch in der DSGVO als Grundsatz der Datensparsamkeit findet, als ausschlaggebend für eine Interessenabwägung zugunsten des Klägers, also des Nutzers des sozialen Netzwerks, an. Der Grundsatz der Datensparsamkeit besagt, dass personenbezogene Daten nur dann verarbeitet werden sollen, wenn dies zur Zweckerreichung tatsächlich

2 OLG München, Urteil vom 8.12.2020, Az.: 18 U 5493/19 Pre.

erforderlich ist. Der BGH sah im Rahmen der DS-RL scheinbar auch kein „beredetes Schweigen“ in Bezug auf die Zulässigkeit der Verwendung von Pseudonymen.
Entsprechend ergibt sich keine durch Auslegung zu korrigierende Unionsrechtswidrigkeit der Normen des TMG. Dieser Einschätzung folgend ergibt sich keine durch Auslegung korrigierte Version des § 13 Abs. 6 S. 1 TMG a.F. Damit ist die betroffene Klarnamenpflicht in den AGB nach Einschätzung des BGH, wie eingangs erörtert, nicht mit den Grundgedanken einer gesetzlichen Regelung vereinbar und mithin nach alter Rechtslage unwirksam.

V. Fazit und Relevanz für wissenschaftliche Einrichtungen

Bemerkenswert im Vergleich der beiden Urteile ist die differenzierende Entscheidung anhand der Auswertung der anzuwendenden Gesetzeslage. Während der BGH unter Zugrundelegung der DS-RL zu dem Ergebnis kommt, dass eine Verwendung von Pseudonymen zumindest im Außenverhältnis zulässig ist, kommt das OLG München in Anwendung der DSGVO zu dem Schluss, dass eine Pflicht zur Verwendung von Klarnamen besteht. Eine klare Entscheidung zum geltenden Recht liegt somit nicht vor.
Ob sich das oberste deutsche Zivilgericht für zukünftige Fälle, in welchen die DSGVO tatsächlich anzuwenden wäre, der Einschätzung des OLG anschließt, ist abzuwarten. Insofern ebenfalls relevant ist, dass auch das TMG mittlerweile durch das neue Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) ersetzt wurde.[3] Hier findet sich allerdings eine dem § 13 Abs. 6 S. 1 TMG a.F. fast wortgleiche Regelung im § 19 Abs. 2 TTDSG. Ob sich daraus eine Übertragung der Argumente aus dem aktuellen Urteil für die mittlerweile geltende Gesetzeslage ergibt, bleibt unklar.

Statt die Frage nach der Klarnamenpflicht in sozialen Netzwerken abschließend zu klären, wirft die aktuelle Entscheidung des BGH neue Fragen auf. Dem Umstand geschuldet, dass nach alter Rechtslage entschieden wurde, ist in Zukunft besonders zu klären, ob die Entscheidung auch nach neuer Rechtslage vergleichbar entschieden würde. In diesem Zuge wäre auch das Verhältnis zwischen TTDSG und DSGVO zu klären. Möglicherweise sind diese Fragen zukünftig auch durch den Gerichtshof der Europäischen Union (EuGH) zu klären.
Auch Hochschulen und wissenschaftliche Einrichtungen sind durch diese Debatte betroffen. Sei es durch den Betrieb eines eigenen sozialen Netzwerks oder die Verwendung solcher. Sei es durch die Benutzerkonten der Mitglieder oder ganzer Einrichtungs-Accounts. Um einer Sperrung durch die Betreiber sozialer Netzwerke zu entgehen, empfiehlt sich vorerst die Verwendung eines Klarnamens. Auf eine zeitnahe höchstrichterliche Klärung der Verpflichtung im Lichte der aktuellen Gesetzgebung ist zu hoffen.

3 Siehe hierzu: John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 5/2021.

Handy weg? EncroChat!

Eine juristische Aufarbeitung des Hacks der verschlüsselten Kommunikationsplattform „EncroChat“

von Justin Rennert

Im März 2020 gelang es den französischen Strafverfolgungsbehörden, die verschlüsselte Kommunikationsplattform „EncroChat“ zu hacken. Die Hintergrundgeschichte dazu liest sich wie ein Krimi. Der vorliegende Beitrag ordnet den EncroChat-Hack juristisch ein und gibt einen kurzen Überblick über die Ermittlungsbefugnisse deutscher Strafverfolgungsbehörden gegenüber den Anbietern von Telekommunikationsdiensten.

I. Einleitung

Das niederländische Unternehmen „EncroChat“ bat Nutzern gegen Entgelt abhörsichere Kommunikation per Direktnachricht oder Voice-over-IP (VoIP) an. Der Dienst erfreute sich in Kreisen der organisierten Kriminalität großer Beliebtheit. EncroChat hatte zum Zeitpunkt des Hacks ca. 60.000 zahlende Abonnenten. Französische Behörden schätzten, dass davon über 90% „in kriminelle Aktivitäten verwickelt seien“. Es ging hier vor allem um den interkontinentalen Rauschgifthandel über Seehäfen wie die in Antwerpen, Rotterdam, Hamburg und Bremerhaven. Sich in Sicherheit wiegend organisierten Drogenhändler ihre Geschäfte über EncroChat einigermaßen unverblümt. So gaben sie Geschäftspartnern ihren Klarnamen preis oder teilten den genauen Ort der nächsten Übergabe mit. Ein Nutzer veranlasste über EncroChat sogar einen Auftragsmord.

Technisch war der Dienst folgendermaßen aufgebaut: EncroChat stellte seinen Nutzern Smartphones zur Verfügung, auf die sowohl ein normales Android-Betriebssystem als auch ein modifiziertes Betriebssystem, das EncroChat OS, aufgespielt waren. Nutzer konnten sich bei jedem Einschaltvorgang entscheiden, ob sie das EncroChat OS oder das reguläre Android nutzen wollen. Auf dem EncroChat OS waren nun wiederum ein eigener Messenger sowie ein eigener VoIP-Dienst installiert. Die Kommunikation über beide Dienste wurde Ende-zu-Ende verschlüsselt und über einen Server in Roubaix, Frankreich, geleitet. Die Geräte selbst verfügten über eine Wipe-Funktion: Mittels Eingabe einer speziellen PIN konnten Nutzer den kompletten Inhalt der Festplatte löschen, um die Daten vor dem Zugriff Dritter zu bewahren.

Der EncroChat-Hack ist eigentlich ein Musterbeispiel europäischer Zusammenarbeit in der Strafverfolgung. Britische Behörden gelangten bei der Aufklärung eines Auftragsmordes im Jahr 2018 in den Besitz mehrerer EncroChat-Smartphones. Sie konnten so den Server in Roubaix ausfindig machen, mit dem die Geräte kommunizierten. Sogleich wiesen die britischen Strafverfolger die französischen Kollegen der Staatsanwaltschaft in Lille auf den Sachverhalt hin. Die französischen Strafverfolger machten sich daraufhin auf den Weg nach Roubaix und analysierten die Funktionsweise des Servers. Das ermöglichte ihnen einige Monate später, einen Trojaner auf den Server zu spielen, der sodann die Endgeräte sämtlicher EncroChat-Nutzer infizierte. Der Dienst war erfolgreich gehackt. Ab diesem Moment konnten die Ermittler jegliche ausgehende und eingehende Kommunikation auf 32.000 Telefonen weltweit mitlesen. Den Ermittlern fielen so insgesamt mehr als 100 Millionen Nachrichten in die Hände. Auf diese erhielten im Rahmen europäischer Rechtshilfeabkommen auch die Staatsanwaltschaften anderer EU-Mitgliedsstaaten Zugriff. In Deutschland kam es bisher aufgrund von Hinweisen in den EncroChat-Datenpaketen zu ca. 2.700 Ermittlungsverfahren. Der Zusatzaufwand für die Justiz ist erheblich. Allein die Stadt Hamburg hat für die Aufarbeitung 28 neue Stellen bei Gerichten und Staatsanwaltschaften eingeplant.

II. Rechtlicher Hintergrund des EncroChat-Hacks

Auf ein Ermittlungsverfahren folgt in vielen Fällen die Anklage vor den Strafgerichten. Hier stellt sich dann die folgende Frage: Dürfen Erkenntnisse aus dem EncroChat-Hack als Beweis für eine Verurteilung verwertet werden? Denn ein kriminaltechnischer Jackpot ist nicht zwangsläufig ein beweisrechtlicher Jackpot. Die Erhebung von Beweisen folgt den strengen gesetzlichen Vorschriften der Strafprozessordnung (StPO). Das Strafrecht wird gemeinhin als „das schärfste Schwert des Staates" bezeichnet. Strafprozessuale Maßnahmen zur Erhebung von Beweisen greifen erheblich in die Grundrechte der Beschuldigten ein – man denke hierbei etwa an die akustische Wohnraumüberwachung. Aus diesem Grund müssen sie von den Gerichten umso strenger und sorgfältiger überprüft werden können. Wenn die Ermittlungsbehörden bei Erhebung des Beweises den einschlägigen gesetzlichen Vorschriften zuwiderhandeln, so kann das dazu führen, dass der Beweis vor Gericht nicht verwertet werden kann. Handelt es sich, wie im Falle EncroChat, um einen grenzüberschreitenden Sachverhalt, werden die zu beachtenden Regelungen noch vielfältiger. So erging seit dem Herbst 2020 eine Vielzahl von Entscheidungen zum EncroChat-Komplex. Für ein Aufhorchen sorgte insbesondere eine Entscheidung des Landgerichts (LG) Berlin aus dem Juli 2021. Das Gericht war der Auffassung, dass die EncroChat-Daten nicht verwertbar seien. Die Überwachung sei ein nicht gerechtfertigter Eingriff in das grundrechtlich geschützte Telekommunikationsgeheimnis sowie das Grundrecht auf Vertraulichkeit und Integrität von IT-Systemen. Zudem verstoße der Hack gegen die StPO. Deren Vorschriften regeln die Zulässigkeit und die Grenzen von Telekommunikationsüberwachung und Online-Durchsuchung für deutsche Ermittlungsbehörden. Das LG Berlin hat auf den von ihm zu entscheidenden Fall also deutsches Strafprozessrecht angewandt. Es argumentierte dabei folgendermaßen: Die Vorschriften der StPO setzen voraus, dass ein Tatverdacht gegen den Betroffenen der Ermittlungsmaßnahme besteht. Der Tatverdacht müsse, so das LG, zeitlich vor der Ermittlungsmaßnahme feststehen. Zum Zeitpunkt des Hacks durch die französischen Behörden habe noch gar kein Tatverdacht gegen konkrete Personen bestanden. Der Tatverdacht ergab sich erst aus den gehackten Daten, habe also nach der Ermittlungsmaßnahme gestanden. Weil das deutsche Recht eine solche zeitliche Abfolge nicht vorsehe, seien die EncroChat-Daten im konkreten Fall unverwertbar.

Diese Rechtsauffassung hat zwar eine (auch öffentlich geführte) Debatte ausgelöst, ist von höheren Gerichten aber einhellig verworfen worden. Die Oberlandesgerichte und auch das in Berlin zuständige ranghöhere Kammergericht (KG) halten die Daten für verwertbar und verurteilen Personen auch auf der Grundlage der Daten. Das KG Berlin verwarf die Entscheidung des LG mit folgender Argumentation: Das deutsche Recht sehe sehr wohl die Möglichkeit vor, dass die Beweiserhebung zeitlich vor dem Verdacht steht. Die EncroChat-Erkenntnisse seien ein sogenannter Zufallsfund. Die Verwertung von Zufallsfunden ist in der StPO ausdrücklich erlaubt (§ 100e Abs. 6 StPO). Dies gelte auch für grenzüberschreitende Sachverhalte. Im Übrigen könne schon die Nutzung eines EncroChat-Telefons einen hinreichenden Verdacht auslösen.

Ähnlich argumentierten auch die Oberlandesgerichte anderer Bundesländer. Dies ist nachvollziehbar und begründet. Der Umstand, dass nach Schätzungen der französischen Behörden 90% der EncroChat-Nutzer in den illegalen Betäubungsmittelhandel involviert gewesen sind, kann die Nutzung eines EncroChat-Telefons schon für sich genommen verdächtig machen. Die Entscheidung des LG Berlin wird daher wohl ein Einzelfall bleiben, hat aber jedenfalls vor Augen geführt, dass die Regelungen zum grenzüberschreitenden Strafprozess in der EU noch nicht hinreichend eindeutig sind. Die EU-Kommission möchte genau eine solche Vereinheitlichung erreichen und hat deshalb den Entwurf einer E-Evidence-Verordnung vorgelegt. Nach dem derzeitigen Entwurf[1] soll es Strafverfolgungsbehörden eines EU-Mitgliedsstaats zukünftig möglich sein, sich direkt an einen Telekommunikations-Diensteanbieter in einem anderen Mitgliedsstaat zu wenden, um bestimmte Daten zu erheben – ohne dass es dabei des Umweges über die Strafverfolgungsbehörden des anderen Mitgliedsstaates bedarf. Derzeit befindet sich die geplante E-Evidence-Verordnung im Trilog-Verfahren zwischen EU-Kommission, Rat der EU und EU-Parlament. Wann die Verordnung geltendes Recht wird, ist noch nicht absehbar.

1 Vorschlag einer E-Evidence-Verordnung, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225 – zuletzt abgerufen am 22.02.2022.

III. Befugnisse der Strafverfolgungsbehörden gegen Telekommunikationsdiensteanbieter

In der EU sind aber auch schon in der Vergangenheit, insb. seit den 1990er-Jahren durchaus relevante Schritte hin zu einer Europäisierung der Strafverfolgung unternommen worden. Man denke hier an die seit 1999 bestehende europäische Polizeibehörde EuroPol oder die seit 2017 bestehende, mit Ermittlungsbefugnissen ausgestattete Europäische Staatsanwaltschaft. Strafverfolgung ist jedoch in ihrem Kern nach wie vor Sache der Nationalstaaten. Insofern lohnt ein kurzer Blick auf die Befugnisse deutscher Ermittlungsbehörden: Welche Maßnahmen können deutsche Ermittlungsbehörden ergreifen, wenn sie den Verdacht haben, dass kriminelle Aktivitäten über ein Kommunikationsnetz gesteuert werden?

1. Telekommunikationsüberwachung, § 100a StPO

Die Strafverfolgungsorgane dürfen die Telekommunikation eines Betroffenen gem. § 100a StPO ohne dessen Wissen überwachen und aufzeichnen. Dies allerdings nur dann, wenn der Verdacht einer schweren Straftat besteht, also beispielsweise bei gewerbsmäßigem Betrug oder Handel mit Betäubungsmittel, aber auch bei Mord und Totschlag, Raub und Erpressung. Telekommunikation umfasst sowohl die Telefonie, aber auch die Kommunikation über Messenger-Dienste und E-Mail sowie sonstige Formen der drahtlosen oder drahtgebundenen Kommunikation. Seitdem die Kommunikation über das Internet zunehmend verschlüsselt wird, ist die Strafverfolgung vor größere Herausforderungen gestellt. Sie müssen verstärkt auf die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) setzen. Dabei werden Daten auf einem Gerät schon vor ihrer Verschlüsselung abgegriffen. Dies geschieht durch das Aufspielen von Trojanern, die sich in ihrer Funktionsweise je nach Zielgerät und Kommunikationsform unterscheiden. Beispielsweise können mittels eines Key-Loggers Eingabevorgänge auf der Tastatur eines Smartphones oder Computers abgefangen werden. Ein solcher Trojaner lag wohl dem EncroChat-Hack zugrunde. Gleichsam wäre es auch möglich, die Audioaufnahmen des Mikrofons eines Laptops abzufangen. Die Quellen-TKÜ ist in der StPO seit 2017 ausdrücklich geregelt.

2. Online-Durchsuchung, § 100b StPO

Im Rahmen der Online-Durchsuchung nach § 100b StPO dürfen die Staatsanwaltschaften ein informationstechnisches System ohne das Wissen des Betroffenen infiltrieren, um jegliche Art von Daten daraus zu erheben. Erfasst sind also nicht bloß Kommunikationsdaten wie bei der Quellen-TKÜ. Die Online-Durchsuchung ist allerdings nur dann erlaubt, wenn der Verdacht einer besonders schweren Straftat besteht. Insofern sind die Voraussetzungen der Erhebung gegenüber der Telekommunikationsüberwachung noch einmal erhöht.

3. Auskunftsansprüche gegen Telekommunikations-Diensteanbieter

Zusätzlich zu den genannten Möglichkeiten der verdeckten Ermittlung und des verdeckten Eingreifens in Kommunikationsvorgänge gibt es für Strafverfolger noch die Möglichkeit, bei Telekommunikations-Diensteanbietern direkt Auskunft über bestimmte Daten zu verlangen. Einen solchen Auskunftsanspruch gibt es sowohl für Bestands- als auch für Verkehrsdaten. Verkehrsdaten sind Daten, die bei der Nutzung eines Telekommunikationsdienstes anfallen (z. B. die Telefonnummer oder dynamische IP-Adresse eines Nutzers, aber auch Dauer und Datum des Kommunikationsvorgangs). Bestandsdaten sind hingegen Daten, die für die Begründung, Änderung oder Beendigung eines Vertrages über Telekommunikationsdienste erforderlich sind (z.B. Name und Anschrift eines DSL-Kunden).

Der Auskunftsanspruch für Verkehrsdaten folgt aus § 100g StPO. Er setzt den Verdacht einer Straftat von erheblicher Bedeutung voraus, insofern sind seine Voraussetzungen geringer als für die TKÜ oder die Online-Durchsuchung. In diesem Zusammenhang ist auch die sog. Vorratsdatenspeicherung von Bedeutung, welche aktuell politisch wieder stark umstritten ist. TK-Diensteanbieter sind verpflichtet, Verkehrsdaten für vier bzw. zehn Wochen auf den eigenen Servern zu speichern. Im Falle eines Verdachts können Strafverfolgungsbehörden in der Theorie dann ihren Auskunftsanspruch geltend machen und in den Besitz der Daten gelangen. Die Pflicht zur Vorratsdatenspeicherung ist in Deutschland allerdings nach einem Urteil des OVG Münster aus 2017 vorläufig ausgesetzt.

Das OVG hielt die Vorratsdatenspeicherung für unvereinbar mit der Rechtsprechung des EuGH. Bundesjustizminister

Marco Buschmann plant aktuell, die Vorratsdatenspeicherung gänzlich aus dem Gesetz zu streichen. [2]

Die Bestandsdatenauskunft ist geregelt unter anderem in § 174 TKG. In der Vergangenheit hat das Bundesverfassungsgericht die Regelungen zur Bestandsdatenauskunft schon mehrfach für verfassungswidrig erklärt, weil sie zu geringe Voraussetzungen für die Auskunftspflicht vorsahen – zuletzt mit Beschluss vom 27.05.2020. Vor diesem Beschluss konnten die Behörden Bestandsdaten jederzeit „für die Erfüllung gesetzlicher Aufgaben" abfragen. Das BVerfG kritisierte diese Formulierung als zu unbestimmt. In dem seither reformierten § 174 TKG ist nun eine präzisere Formulierung gewählt. Die Bestandsdatenauskunft ist nunmehr unter anderem dann zulässig, wenn „zureichende tatsächliche Anhaltspunkte für eine Straftat oder Ordnungswidrigkeit vorliegen" oder eine „Gefahr für die öffentliche Sicherheit" besteht.

IV. Fazit

Der EncroChat-Hack ist eine Erfolgsgeschichte der europäischen Zusammenarbeit in der Strafverfolgung. Die Entscheidungen deutscher Gerichte zur Verwertbarkeit der EncroChat-Erkenntnisse sind nur folgerichtig. In angemessener Weise übertragen sie die deutschen Regelungen zum Zufallsfund von Beweisen auf grenzüberschreitende Sachverhalte. In diesem Zusammenhang lohnt auch ein Blick auf die geplante EU-E-Evidence-Verordnung, von der eine noch stärkere Vereinheitlichung der grenzüberschreitenden Beweisübermittlung ausgehen wird. Der Zugriff auf die Daten ist aber auch eine kriminaltechnische Erfolgsgeschichte. Die Strafverfolgungsbehörden haben gezeigt, dass sie Zugriff auf die Kommunikation mutmaßlicher Straftäter nehmen können, selbst wenn diese verschlüsselt ist. Wissenschaftlich dürfte der EncroChat-Hack vor allem für Informatiker sowie Kriminaltechniker interessant sein. Aber auch juristisch birgt der Hack, wie hier dargestellt, einige Fragestellungen.

2 https://www.spiegel.de/netzwelt/netzpolitik/marco-buschmann-bundesjustizminister-will-vorratsdatenspeicherung-kippen-a-9de4fead-9873-4230-b342-7b19def9f425 - abgerufen am 22.02.2022.

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