§ 23
Der strafrechtliche Schutz von Daten durch § 303a StGB und seine Auswirkungen auf ein Datenverkehrsrecht

I. Einführung

Die Frage nach dem Eigentum oder der Inhaberschaft sonstiger Rechte an Daten ist im Zeitalter von Big Data zentral. Die **rechtliche Zuordnung von Daten** ist **zurzeit vollkommen unklar**, was aufgrund der immensen Bedeutung von Daten und Rechten an Daten in der heutigen Informationsgesellschaft als äußerst unbefriedigend empfunden werden muss und zu gravierender Rechtsunsicherheit für die Betroffenen führt. Sowohl Privatpersonen als auch Unternehmen arbeiten tagtäglich mit großen Mengen von Daten. Für diese ist selbst mit juristischem Rat nicht ersichtlich, ob und, wenn ja, auf welche Weise ihre Daten rechtlich geschützt sind. Ebenso schwierig ist es, festzustellen, ob Dritten Rechte an den betroffenen Daten zustehen. Auch der Umfang solcher Rechte ist – soweit sie bestehen – momentan kaum zu bestimmen. Erschwerend hinzu kommt noch, dass die Gerichte auf deutscher und europäischer Ebene unterschiedliche Lösungsansätze vertreten. 1

Aufgrund der enormen wirtschaftlichen Bedeutung von Daten insbesondere im Hinblick auf Big-Data-Anwendungen ist zu befürchten, dass diese **Unsicherheiten** große **Investitionshemmnisse** darstellen. Das Risiko, sich zivil- oder strafrechtlichen Ansprüchen auszusetzen oder selbst keine gesicherte Rechtsposition in Bezug auf Daten zu erlangen, ist unkalkulierbar. Deswegen sollte eine möglichst baldige Klärung der bestehenden Rechtsfragen angestrebt werden. Im Folgenden werden daher mögliche Lösungsansätze aufgezeigt, die erstaunlicherweise über die in der Praxis wenig angewendete Strafvorschrift des § 303a StGB laufen, womit sich die Frage stellt, ob § 303a StGB als Tor für ein **neues Datenverkehrsrecht** genutzt werden kann[1]. 2

1 Es freut den Verfasser, diese Überlegungen einem der großen Nestoren des Datenrechts widmen zu können. *Jochen Schneider* hat wie kaum ein anderer das

II. Warum das traditionelle Datenrecht versagt

3 Ansätze zu einem Datenrecht gibt es schon. Sie scheitern aber sämtlich bei der originären Zuordnung von Ausschließlichkeitsrechten an Daten.

4 Der als Ausschließlichkeitsrecht und subjektiv-rechtliche Rechtsposition ausgestaltete[1] **Schutz des Datenbankherstellers (§ 87a UrhG)** begründet nur den Schutz vor Vervielfältigung, Verbreitung und öffentlicher Wiedergabe, nicht jedoch ein **eigentumsähnliches Vollrecht**. Auch die Erschöpfungswirkung an körperlichen Vervielfältigungsstücken der Datenbank[2] zeigt, dass gerade nicht der Schutz von Daten bezweckt wird, sondern der des Dateninhalts. Im Vordergrund stehen der Investitionsschutz und die wirtschaftliche Verwertung der Investition. Wie andere Leistungsschutzrechte oder gewerbliche Schutzrechte hat der Datenbankschutz nur eine begrenzte Schutzdauer (nämlich 15 Jahre, § 87d UrhG). Weiterhin umfasst er auch Vervielfältigungen von Daten, die sich durch gleichen Inhalt auszeichnen, schließt aber Dritte nicht von der bloßen Benutzung (Abfrage) der Informationen aus. Dies zusammengenommen zeigt, dass mit der Regelung für Datenbanken ein spezieller Investitionsschutz geschaffen werden sollte, der vor wirtschaftlicher Ausbeutung fremder Leistung schützt, nicht aber eine rechtliche Zuordnung von Daten zu einer Person. Der Sui-generis-Schutz schafft eine zusätzliche abstrakte Ebene, die in einer systematischen Anordnung von Inhalten besteht, jedoch selbst lediglich inhaltlicher Natur ist.

5 Das **Datenschutzrecht** schützt nur dem Namen nach „Daten". Tatsächlich **geht es um** den dargestellten Inhalt, sprich die **Information, welche sich mit einer Person in Beziehung bringen** lässt. Dies lässt § 3 Abs. 1 BDSG erkennen, der personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" definiert. Personenbezogene Daten im Sinne des Datenschutzrechts sind also „Angaben" und damit Inhalte, und dürfen nicht mit Daten im technischen Sinne verwechselt werden. Nur solche Daten, die einen Bezug zu einer natürlichen Person aufweisen oder die sich mit zusätzlichen Informationen auf diese beziehen lassen, können die Anwendbarkeit des BDSG begründen. Es handelt sich im Ergebnis also um ein Persönlichkeitsrecht. Der Schutz personenbezogener Da-

---

deutsche und europäische Datenrecht beeinflusst; auch er hat den Schlüssel zur Etablierung eines Datenverkehrsrechts nicht gefunden. Von daher freut es den Verfasser, ihn in München nach seinem Geburtstag sitzen zu sehen – in Erfüllung seiner Ehrenpflicht, jeden Festschriftbeitrag lesen zu müssen. Schau mer mal, was er denkt! – Der Verfasser freut sich auf die Rückmeldung von *Jochen Schneider*, die bajuwarisch-nordische Diskussion über das Datenrecht bei Weizen und Pils. – Der Beitrag entstand im Rahmen eines BMWi-Forschungsprojekts zu Rechtsfragen von Big Data; s. auch *Hoeren*, MMR 2013, 486.

1 Vgl. BGH, MMR 1999, 470 (472); *Gaster* in Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 7.6 Rz. 75 f.

2 *Gaster*, Der Rechtsschutz von Datenbanken, S. 131 Rz. 522 ff.; *Dreier* in Dreier/Schulze, UrhG, § 87b Rz. 18; *Thum* in Wandtke/Bullinger, UrhR, § 87b Rz. 58.

ten wird an vielen Stellen über die Beziehung zwischen der Information und dem Datum geregelt. Es entstehen aber durch das Datenschutzrecht keine über eine Information vermittelten Beziehungen einer Person zu einer Sache, sondern direkt zu Daten. So können beispielsweise nach § 35 BDSG Löschungs- oder Berichtigungsansprüche gegen eine verarbeitende Stelle unabhängig davon geltend gemacht werden, in welcher Form die Daten vorhanden sind. Auch Auskunftsansprüche (z.B. aus § 34 BDSG) gewähren dem Betroffenen immer nur das Recht, Daten vorgelegt zu bekommen, die mit den gespeicherten Daten inhaltsgleich sind. Das umfasst zwar beispielsweise auch die Auskunft über die Bezeichnung der Datei, in der die personenbezogenen Daten gespeichert sind[1], der Betroffene erhält aber nicht das Recht auf Zugang zu dem Hauptspeichermedium, wie etwa dem Server der verarbeitenden Stelle. Das Datenschutzrecht schafft damit eine rechtliche Verantwortlichkeit für Daten. Es darf aber nicht dahingehend missverstanden werden, dass der Betroffene Ausschließlichkeitsrechte an den einzelnen Datensätzen im Sinne eines „Eigentums" besitzt.

Die **Rechtsprechung** geht davon aus, dass ein **Datenträger** mit den darauf verkörperten Daten **eigentumsfähig** ist. So hat das OLG Karlsruhe[2] eine Eigentumsfähigkeit von Daten im Rahmen von **§ 823 Abs. 1 BGB** bejaht[3]. Der Datenträger mit den darauf verkörperten Daten sei jedenfalls eine körperliche Sache[4]. Zwar könne die Information, die in diesen Daten repräsentiert ist, wegen ihrer immateriellen Natur nicht Schutzgut einer Norm gegen die Beschädigung der materiellen Substanz sein. Jedoch sei deswegen von einer Verletzung des Eigentums auszugehen, weil der Eigentümer durch den Eingriff gehindert werde, mit der Sache seinem Wunsch entsprechend zu verfahren. Diese Argumentation löst aber nur die Frage nach einer Eigentumsfähigkeit datenträgergebundener Daten und schafft eher ein Eigentum am Datenträger als eine Begründung für ein Eigentum an Daten. 6

Im Übrigen wird **zum Teil vertreten**, dass sich aus **§ 823 Abs. 1 BGB als sonstiges Recht** auch ein Recht am eigenen Datenbestand herleiten lasse[5]. Ein solches Recht benötigt freilich zur Legitimation eine gewisse eigenständige Bedeutung neben anderen Rechten. Werden Daten auf einem Datenträger unbrauchbar gemacht, so ist – sogar weitergehender als nach der Ansicht des *OLG* Karlsruhe[6] – von einer Substanzverletzung an dem 7

1 HessVGH, RDV 1991, 187; *Gola/Schomerus*, BDSG, § 34 Rz. 9.
2 OLG Karlsruhe, NJW 1996, 200.
3 S. dazu auch den Beitrag von *Bartsch*, § 22; a.A. LG Konstanz, NJW 1996, 2662; s. auch *Gerstenberg*, NJW 1956, 540.
4 *Jickeli/Stieper* in Staudinger, BGB, § 90 Rz. 12; *Redeker*, NJW 2008, 2684 (2685).
5 S. dazu BGH, NJW 1996, 2924 (2925); ähnlich auch *Meyer/Wehlau*, NJW 1998, 1585 (1588); vgl. auch *Bartsch*, § 22 Rz. 17 ff.
6 OLG Karlsruhe, CR 1987, 19.

Datenträger auszugehen, da dieser nachhaltig physisch verändert wurde[1]. Mit diesem Rückgriff auf das Eigentum am Datenträger werden allerdings **viele Probleme**, die bei vernetzten Datenbeständen auftreten, **nicht gelöst**[2]. Bedeutsam sind besonders die Fälle, in denen der wirtschaftliche Schaden nicht beim Eigentümer des Datenträgers entsteht, weil nicht er, sondern ein Dritter den wirtschaftlichen Umgang mit der Information pflegt. Für solche Fälle hat das Recht am eigenen Datenbestand durchaus seine Berechtigung. Allerdings zeichnen sich „sonstige Rechte" i.S.d. § 823 BGB dadurch aus, dass sie eine den ausdrücklich normierten Rechten entsprechende Ausschluss- und Nutzungsfunktion besitzen[3]. Genauer stellt sich die **Frage, wer unter Ausschluss Dritter an einem Datenbestand berechtigt ist**. Das Recht am eigenen Datenbestand ist daher eine Hilfskonstruktion, die zunächst mehr Probleme aufwirft als löst.

III. Der Weg über § 303a StGB

8 Möglicherweise können Grundgedanken aus dem Strafrecht zur Beantwortung der Frage, wem Daten gehören, beitragen[4]. Im Strafrecht besteht **im Rahmen des § 303a StGB** die **Notwendigkeit, die Zuordnung** der Daten zum Berechtigten zu definieren. Diese Zuordnung wird zum großen Teil so verstanden, dass an den Daten ein Vollrecht analog § 903 BGB entstehe[5]. Anknüpfungspunkte für die Zuordnung eines solchen Rechts sollen u.a. die nach den Regeln des Zivilrechts zu qualifizierenden dinglichen und obligatorischen Rechte an Datenträgern sein, also die durch das Herstellen der Daten vermittelte Urheberschaft (unter Rückgriff auf § 950 BGB sowie die Grundsätze in §§ 4, 69a ff. UrhG), und die Inhaberschaft an den gespeicherten Originaldaten im Rahmen einer Auftragsdatenverarbeitung[6].

1. Zuordnung nach der persönlichen Betroffenheit durch Daten

9 Dieser Ansatz wurde in der Literatur zu § 303a StGB schon kurze Zeit nach der Entstehung der Vorschrift diskutiert[7]. Im Zuge der Entwicklung in der Wissenschaft wurde aber richtigerweise die **Unzweckmäßigkeit des Kriteriums** der Betroffenheit für die Herrschaftszuordnung erkannt. Zwar gibt eine Formulierung in den Gesetzesmaterialien eine entspre-

1 OLG Oldenburg, MDR 2012, 403; *Meyer/Wehlau*, NJW 1998, 1585 (1588).
2 *Meyer/Wehlau*, NJW 1998, 1585 (1588); s. auch die Beispiele bei *Bartsch*, § 22 Rz. 10 ff.
3 *Wagner* in MünchKommBGB, § 823 Rz. 143.
4 Vgl. hierzu eingehend *Hoeren*, MMR 2013, 486 (486 ff.).
5 *Hilgendorf*, JuS 1996, 890 (890); *Stree/Hecker* in Schönke/Schröder, StGB, § 303a Rz. 3; *Welp*, IuR 1988, 443 (448).
6 Ähnlich BayObLG, CR 1993, 779; *Bär* in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, § 303a Rz. 13; *Cornelius* in Kilian/Heussen, Computerrechts-Handbuch, Teil 10 Rz. 180; *Wolff* in Leipziger Kommentar, § 303a Rz. 10 ff.
7 *Welp*, IuR 1988, 443 (448) m.w.N. in Fn. 46.

chende Auslegung her, doch soll im Hinblick auf das Rechtsgut des § 303a StGB gerade die **Verfügungsbefugnis über die Integrität der Daten von ihrem Inhalt getrennt** werden[1]. Das durch die Strafnorm geschützte Rechtsgut ist die Verwendbarkeit der Daten durch den Berechtigten[2]. Eine Zuordnung nach Betroffenheit würde aber gerade den Inhalt und die Zuordnung gleichstellen.

Eine Zuordnung gestützt auf das Kriterium der Betroffenheit **ließe sich auch nicht mit dem Datenschutzrecht in Einklang bringen**. Die datenschutzrechtlichen Vorschriften sollen die Einschränkungen, denen die datenverarbeitende Stelle im Umgang mit den Daten (im technischen Sinne) unterliegt, abschließend regeln. Nur in dem dort geregelten Umfang sollen Beschränkungen bestehen. Erfolgte die Zuordnung im Rahmen des § 303a StGB aufgrund der Betroffenheit, so würde die gesetzliche Erlaubnis zur Verarbeitung personenbezogener Daten einem Eingriff in das „Dateneigentum" des Betroffen gleichkommen. Auch ergibt sich die nähere Beziehung zum Sacheigentum im Gegensatz zum Persönlichkeitsrecht aus der systematischen Stellung des § 303a StGB in den Eigentumsdelikten, direkt nach der Sachbeschädigung[3]. 10

2. Zuordnung nach Sacheigentum am Datenträger

Teilweise wird angenommen, die Zuordnung von Daten zu einer Person im Rahmen von § 303a StGB folge direkt den dinglichen Rechten am Datenträger[4]. Dieser **Ansatz verkennt**, dass der **Eigentümer** von Datenspeichern, etwa von Servern, **regelmäßig in keiner Beziehung zu den Daten** steht, weil er nur Dritten den Speicherplatz zur Verfügung stellt. Wer etwa als Host-Provider nur eingeschränkt für den Inhalt von Daten verantwortlich ist[5], kann nicht einziger Verfügungsberechtigter über die Daten im Sinne eines strafrechtlichen Eigentumsdelikts sein. Schon aus der Laiensphäre kann die Wertung des § 303a StGB nicht bedeuten, dass der Nutzer eines Host-Dienstes die Verfügungsbefugnis über „seine" Daten nur aufgrund der schuldrechtlichen Beziehung zum Serverbetreiber besitzt[6]. Das zeigt sich auch im Vergleich mit der Situation zwischen dem Eigentümer einer Mietwohnung und den Gegenständen, die der Mieter in der Wohnung aufbewahrt. 11

Zudem soll § 303a StGB der Berechtigung an den Daten eine eigenständige Bedeutung geben, ansonsten hätte der Tatbestand auch an eine Sachbeschädigung durch Verändern von gespeicherten Daten anknüpfen kön- 12

1 *Hilgendorf*, JuS 1996, 890 (892); *Welp*, IuR 1988, 443 (448).
2 *Hilgendorf*, JuS 1996, 890 (890); *Welp*, IuR 1988, 443 (448).
3 *Haft*, NStZ 1987, 6 (10).
4 *Stree/Hecker* in Schönke/Schröder, StGB, § 303a Rz. 3; *Wieck-Noodt* in MünchKommStGB, § 303a Rz. 10.
5 *Hoeren* in Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 18.2 Rz. 124.
6 Wie aber angedeutet von *Wieck-Noodt* in MünchKommStGB, § 303a Rz. 10.

nen. Um die Interessen des Datenverkehrs zu wahren, müssen auch Datenträgereigentum und Dateneigentum auseinanderfallen können[1].

13 Das Kriterium der Eigentümerschaft am Speichermedium kann deshalb höchstens als eines von mehreren Kriterien wirken, um die Eigentumsverhältnisse an Daten zu klären.

3. Zuordnung nach Schaffensprozess

14 Als Zuordnungskriterium wird weiterhin der Prozess der **Entstehung von Daten** diskutiert. In Frage kommen diesbezüglich die geistige oder die technische „Urheberschaft"[2].

15 Die **geistige Urheberschaft** knüpft an den Dateninhalt an. Gegen eine Beurteilung der Datenberechtigung auf der Grundlage geistiger Urheberschaft wird **eingewandt**, dass damit § 303a StGB in eine **Erweiterung des Urheberrechtsschutzes** verwandelt und so eine weitreichende Pönalisierung inhaltsverändernden Verhaltens außerhalb der §§ 4, 69a ff., 106 ff. UrhG geschaffen würde, die vom Regime des Urheberrechts nicht vorgesehen ist[3]. Abgesehen von diesem überzeugenden wertenden Argument erscheint das Kriterium der geistigen Urheberschaft kaum praktikabel. Für eine quasi-dingliche Rechtsposition ist es problematisch, vollständig auf ein Publizitätsmoment zu verzichten. Jede Kopie des Inhalts von Daten oder auch nur die Eingabe eines zuvor analog verkörperten Gedankeninhalts in digitale Daten würde ferner dem ursprünglichen Urheber des Inhalts zufallen. Parallel zu der Zuweisung nach dem Eigentum am Speichermedium würde wieder die Eigenständigkeit der Daten neben Medium und Inhalt in Frage gestellt. Damit ließe sich die spezifische Regelung für Daten nicht erklären.

16 Als dogmatisch einwandfreies und **operabelstes Kriterium** gilt der Prozess der **technischen Herstellung der Daten**. *Welp* prägte dafür den Begriff des „Skripturakts"[4]. „Skribent" und damit originär Berechtigter an den Daten soll derjenige sein, der durch Eingabe oder Ausführung eines Programms Daten selbst erstellt[5]. Dieses Kriterium ist insofern dogmatisch und praktisch brauchbar, als es gerade an die spezifische Dateneigenschaft anknüpft. Der „Skribent" ist der technische „Ersteller" der Daten, zunächst unabhängig davon, auf wessen Medium die Speicherung geschieht und wer geistig den Inhalt geprägt hat. Auch innerhalb eines Arbeits- oder Dienstverhältnisses, in dem Daten im Auftrag erstellt werden, soll zunächst der Auftragnehmer Berechtigter sein, bis er die Daten

1 *Hilgendorf*, JuS 1996, 890 (893).
2 *Hilgendorf*, JuS 1996, 890 (892).
3 *Hilgendorf*, JuS 1996, 890 (893).
4 OLG Nürnberg v. 23.1.2013 – 1 Ws 445/12; *Welp*, IuR 1988, 443 (447).
5 *Welp*, IuR 1988, 443 (447).

ausgehändigt hat[1]. Letzteres ist zwar umstritten[2], im Ergebnis aber wohl richtig, denn zum einen ist so die eindeutige Zuordnung gewährleistet und zum anderen soll § 303a StGB nicht zu einer weiten Kriminalisierung von Vertragsbrüchen führen. Werden hingegen übermittelte Daten im Auftrag verarbeitet, soll der ursprüngliche Inhaber der Originaldaten verfügungsbefugt bleiben[3].

4. Verhältnis von Medien- und Dateneigentum

Maßgebendes Kriterium für die Entstehung einer originären Zuordnung der Daten könnte also der Skripturakt sein[4]. Wie oben bereits angedeutet, **könnten damit das Eigentum an dem Speichermedium und das „Dateneigentum" auseinanderfallen**. Dieses Ergebnis ist mit Hinblick auf Hosting-Verhältnisse und Auftragsverhältnisse auch einleuchtend. Wenn aber die Speicherung ohne oder gegen den Willen des Medieneigentümers erfolgt, kommt es zu einer Konfliktsituation der Rechte[5]. Fraglich ist, ob diese direkt auf der Ebene des Entstehens des Dateneigentums oder im Nachhinein zu lösen ist. 17

a) Skribent als Dateneigentümer

Da das Sacheigentum zunächst von der Rechtsordnung stärker und unmittelbarer geschützt ist, liegt es nahe, dass der Eigentümer eines Datenspeichers es nicht uneingeschränkt dulden muss, wenn sein Eigentum durch die Rechte Dritter an Daten beeinträchtigt wird[6]. Es erscheint aber systemwidrig, ihn in allen Fällen der Verletzung seines Eigentums durch fremde Datenskriptur als alleinigen Dateninhaber anzusehen[7]. Der Skribent könnte dann nämlich nur durch Willensakt des Eigentümers Dateneigentum durch Erzeugung entstehen lassen. Somit wäre wiederum das Medieneigentum das grundlegende Zuordnungskriterium. Konsequent wäre es daher, die Dateninhaberschaft auch in dem Fall **immer dem Skribenten zuzuordnen**, in dem er vorsätzlich auf fremden Speichermedien Daten ablegt, dem **Eigentümer** jedoch gleichzeitig **nur zivilrechtliche Unterlassungs- und Beseitigungsansprüche** aufgrund seines Sacheigentums zuzuerkennen[8]. Dass im Endeffekt die Rechtekollision wohl grundsätzlich über derartige Ansprüche zu lösen sein wird, ist jedenfalls syste- 18

1 OLG Nürnberg v. 23.1.2013 – 1 Ws 445/12.
2 *Fischer/Schwarz/Dreher* et al., StGB, § 303a Rz. 6.
3 Ähnlich BayObLG, CR 1993, 779; *Bär* in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, § 303a StGB Rz. 13; *Cornelius* in Kilian/Heussen, Computerrechts-Handbuch, Teil 10 Rz. 180; *Wolff* in Leipziger Kommentar, § 303a Rz. 10 ff.
4 Vgl. auch *Kühl* in Lackner/Kühl, StGB, § 303a Rz. 4; *Rengier*, Strafrecht, Besonderer Teil, Bd. 1 Vermögensdelikte, § 26 Rz. 7.
5 *Welp*, IuR 1988, 443 (448).
6 *Welp*, IuR 1988, 443 (448).
7 *Welp*, IuR 1988, 443 (448).
8 *Hilgendorf*, JuS 1996, 890 (893).

matisch folgerichtig, wenn man dem „Dateneigentum" einen dinglichen Charakter zuspricht.

b) Ausnahmen

19 Allerdings müssen von diesem Grundsatz **wertungsgerechte Ausnahmen** gelten. Es kann nicht sein, dass das Recht aus § 903 BGB, mit der Sache nach Belieben zu verfahren, durch eine reine Abspeicherung einer Datei auf einen Datenträger massiv beeinträchtigt werden kann, ohne dass der Eigentümer die Entstehung der Daten nicht zumindest mit veranlasst hat. Man denke nur daran, diesen Grundsatz auf in ein System eingeschleuste Daten anzuwenden. Dann müsste etwa der Nutzer eines PCs vor Entfernen einer Schadsoftware den Angreifer zuvor erfolgreich verklagen, wenn er sich nicht auf Rechtfertigungsgründe (§ 904 BGB) berufen kann. In Ausnahmefällen muss die Verfügungsbefugnis an Daten also auch originär beim Eigentümer des Mediums entstehen. Ein solcher Ausnahmefall ist immer dann **anzunehmen, wenn der Eigentümer die Skriptur nicht selbst in irgendeiner Form mitveranlasst hat**. Dabei kommt es auf seinen Willen nicht an. Eine Mitveranlassung scheidet aber zumindest dann aus, wenn etwa die Sache abhandengekommen ist (§ 935 BGB) oder die Skriptur durch Einbruch in ein System erfolgt ist. Letzteres gebietet schon das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das die Verfügungsgewalt des Systeminhabers sicherstellen soll[1].

c) Automatische Skriptur

20 Als problematisch könnte sich noch die bereits angesprochene automatische Skriptur erweisen. Im Grundsatz ist eindeutig, dass die Zuordnung zum Skribenten auch dann erfolgen muss, wenn dieser Programme ausführt, die Daten erstellen oder eine Dateneinspeisung selbst bewirken[2]. Das gilt auch für profan-physische Akte, wie dem Betreiben einer Mikrowelle mit Datenspeicher oder dem Auslösen einer Digitalkamera. Fraglich ist aber, wie viel **Anteil an der Skriptur** durch einen vorprogrammierten Prozess eine Person noch hat, die nur einen unwesentlichen Teil dieses Prozesses, aber damit das Resultat beeinflusst. Als Beispiel sei eine umfangreiche Datenbank genannt, in der durch einen Bearbeiter unter vielen einzelne Bestandteile verändert oder eingebracht werden. In solchen Fällen prozessual festgelegter Skriptur muss nach Wesentlichkeit des Beeinflussungsmoments abgegrenzt werden, wobei auch die Grundsätze zur Veranlassung und dem Medieneigentum eine Rolle spielen können.

1 *Polenz* in Kilian/Heussen, Computerrechts-Handbuch, Teil 13 Rz. 36.
2 *Welp*, IuR 1988, 443 (447).

5. Reichweite der Datenverfügungsbefugnis

Die Datenverfügungsbefugnis erfasst zunächst jedes einzelne Datum und auch zusammenhängende Datenstrukturen. Anders als bei Sachen kann jedoch die Eingrenzung eines Datums nicht einfach an einem Stoff festgemacht werden. Wie das oben besprochene Urteil des EuGH zeigt, ist es vertretbar, dass der rechtliche Zuweisungsgehalt von Daten nicht endet, wenn deren Inhalt vervielfältigt wird. Das zeigt die Gleichstellung der Weitergabe von Werkstücken in körperlicher und unkörperlicher Form. **Fraglich** ist also, ob die **Kopie einer Datei** ebenfalls in den Zuweisungsbereich der ursprünglichen Datei fällt. 21

Hilgendorf sieht jedenfalls bezüglich § 303a StGB die Kopie nicht von der Verfügungsbefugnis des Berechtigten erfasst[1]. Allerdings soll kein Eingriff in das Rechtsgut des § 303a StGB vorliegen, wenn eine „fremde" Datei auf einem eigenen Medium gelöscht wird und der Berechtigte eine inhaltsgleiche Kopie zurückbehalten hat[2]. Das lässt sich damit erklären, dass der Berechtigte in die Veränderung der weitergegebenen Version eingewilligt hat oder dass die Versagung einer solchen Einwilligung in einem Auftragsverhältnis treuwidrig sein kann. Das Dateneigentum an Kopien kann nicht generell anhand der Kopie des Inhalts festgelegt werden. Insoweit ist die Zuweisung der Datenberechtigung getrennt von den Grundsätzen der Erschöpfung bei Werkstücken zu betrachten. Vielmehr gelten **auch hier die Kriterien der Skriptur** und der Veranlassung. Werden Daten in demselben System und auf demselben Datenträger „kopiert", wird wohl nicht der Kopierende, sondern der **ursprüngliche Ersteller** der Berechtigte bleiben. Werden sie auf ein anderes Medium kopiert, ist nach dem Kopiervorgang zu unterscheiden. Entweder werden Daten direkt auf ein Medium kopiert, das dann weitergegeben wird (z.B. eine CD-Rom), oder in einem Netz verschoben. In diesen Fällen ist Skribent der Ersteller der Kopie bzw. der Absender. **Mit der Überlassung verfügt er aber über sein Recht** an den Daten zugunsten des **Empfängers**, so dass dieser mit Entgegennahme die **Berechtigung erwirbt**. Werden die Daten allerdings zum Abruf bereitgestellt und direkt vom Empfänger selbst kopiert, dann ist jedenfalls er selbst Skribent und damit originär Berechtigter. 22

Die Verfügungsbefugnis endet mit der Aufgabe der Daten, also wenn der Berechtigte über einen längeren Zeitraum kein Interesse mehr an ihnen zeigt[3]. Dann wird die Inhaberschaft wohl am ehesten dem Medieneigentümer zufallen. 23

1 *Hilgendorf*, JuS 1996, 890 (890).
2 *Hilgendorf*, JuS 1996, 890 (893).
3 *Hilgendorf*, JuS 1996, 890 (894).

IV. Fazit

24 Im Gegensatz zum Zivilrecht, dem in Bezug auf die Frage nach dem Zuweisungsgehalt des Eigentums eine viel größere Rolle zukommt, gibt es im Strafrecht die Regelung des § 303a StGB, die sich explizit auf Daten als geschütztes Gut bezieht. Zwar spricht einiges dafür, die Zuordnung der Daten im Rahmen des § 303a StGB anhand des Skripturaktes vorzunehmen. Wie die vorherige Darstellung allerdings verdeutlicht hat, herrscht diesbezüglich eine erhebliche Rechtsunsicherheit. Dies gilt vor allem im Zivilrecht, weil es dort keine Norm gibt, die sich explizit mit Daten befasst. Deshalb ist es umso bedeutender, im bestehenden Geflecht aller rechtlichen Normen Lösungen zu finden.