den Standardprogramme stand und fiel. Der Hinweis auf die nicht übernommene Mitverantwortung befreit daher H bestenfalls von einer Verpflichtung zum Schadensersatz. Eine solche Verpflichtung läßt sich, wie oben nachgewiesen, ohnehin nicht aus der für den Einwendungsdurchgriff ausreichenden wirtschaftlichen Einheit ableiten. Hinzutreten muß vielmehr eine schuldhafte Verletzung vertraglicher Pflichten oder die Verletzung eines Garantieversprechens.

Trotz der vorstehend aufgezeigten Möglichkeit eines Einwendungsdurchgriffs ist jedem Gewerbetreibenden, welcher sich gezwungen sieht, die Anschaffung einer Datenverarbeitungsanlage in den Kauf der Hardware und in die Bestellung der Software auf verschiedene Unternehmen aufzuteilen, anzuraten, der bestehenden tatsächlichen Abhängigkeit in der Ausgestaltung der Verträge ausdrücklich Rechnung zu tragen. Wer jedoch in blindem Vertrauen auf den Ruf und die Leistungsfähigkeit seiner Vertragspartner gehandelt hat, ist darauf angewiesen, ausreichende Verbindungselemente nachzuweisen. Hierfür soll dieser Beitrag eine Unterstützung sein.

Die strafbare Fälschung beweiserheblicher Daten (§ 269 StGB)

Zur „hypothetischen" Subsumtion beweiserheblicher Daten unter den Urkundenbegriff des § 267 StGB

Michael Rösler

1. Einführung

Durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) wurde 1986 ein neuer Tatbestand § 269[1] in das Strafgesetzbuch eingefügt.[2] Ziel dieser Maßnahme war es, Datenfälschungen — einen Teilbereich möglicher Computermanipulationen — unter Strafe zu stellen. Das Reformvorhaben wurde seit Anfang der siebziger Jahre diskutiert. Das Schwergewicht der Diskussion betraf jedoch nicht die Ausgestaltung der Tatbestände, sondern die Typologisierung der Computerkriminalität und den Umfang ihrer Schädlichkeit für die Allgemeinheit. Die Vernachlässigung der systematischen Arbeit für die Entwicklung von Rechtsgütern, Tatbeständen und Gesetzessystematik könnte sich zum Nachteil des strafrechtlichen Schutzes gegen Computerkriminalität ausgewirkt haben.[3] Ob dem § 269 n.F. daher eine praktische Bedeutung zukommt, hängt nicht nur von der Anzahl der einschlägigen Fälle ab. Der Tatbestand muß für die Praxis auch handhabbar sein. Für die kriminalistischen und kriminologischen Probleme sei auf die Literaturhinweise (Abschnitt 8) verwiesen.

2. Schützt § 269 ein neues Rechtsgut?

Geschütztes Rechtsgut des 23. Abschnitts im StGB ist die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs.[4] Im Vordergrund steht das Vertrauen in die Echtheit und Unverfälschtheit der Urkunde, also die Sicherheit der einem Menschen zugerechneten Erklärung. Dagegen genießt das Vertrauen in die inhaltliche Wahrheit keinen Schutz. Der Gesetzgeber hob hervor, daß er dieses Rechtsgut nicht ändern wollte. Die überwiegende Meinung stimmt dem Gesetzgeber

1. Soweit nicht besonders erwähnt, beziehen sich zitierte Paragraphen auf das Strafgesetzbuch. Verkürzt zitierte Literatur ist in den Literaturhinweisen mit vollständigem Titel aufgeführt worden.

2. **Bundesgesetzblatt Teil I** S. 721. Dokumentation des Gesetzgebungsverfahrens m.w.N. **Möhrenschlager**, Wistra 1986, 123 ff.

3. Vgl. auch die Kritik von **Dreher/Tröndle** § 269 Rn. 1, 5 und **Systematischer Kommentar/Samson** Vor § 267 Rn. 14

4. So **BGHSt** 2, 50, 52. **Schönke/Schröder/Cramer** § 267 Rn. 1 m.w.N. **Wessels** Strafrecht Besonderer Teil, Band 1, 10. Aufl. 1986, § 18 I 1.

zu.[5] Es ergeben sich aus § 269 keine Anhaltspunkte für eine andere Auffassung. Daher wird die Zuverlässigkeit und Sicherheit des Rechts- und Beweisverkehrs dort geschützt, wo sich dieser der EDV als technisches Hilfsmittel bedient.

3. Die „beweiserheblichen" Daten des § 269

a) Daten der Informationsverarbeitung

Als Tatobjekt werden Daten genannt. Zwar liegt in § 202a II eine Legaldefinition des Begriffs vor, doch ist diese nach überwiegender Meinung nur auf diejenigen Tatbestände anzuwenden, welche explizit auf § 202a II verweisen.[6] Unter „Daten" versteht man in der Informatik allgemein **Zeichen oder kontinuierliche Funktionen, die zum Zweck der Verarbeitung Informationen — auf Grund bekannter oder unterstellter Vereinbarungen in einer für eine DVA erkennbare Weise codiert — darstellen.** Dabei wird heute der Verarbeitungszweck nicht mehr betont.[7] Mithin umfaßt dieser Begriff jede Information, die sich in einer für die DVA erkennbar codieren läßt. Insbesondere spielt keine Rolle, auf welche Weise die Informationen gespeichert oder verarbeitet werden, oder ob die Daten tatsächlich weiter verarbeitet werden.[8]

Die Frage, ob nur visuell nicht wahrnehmbar gespeicherte Daten durch § 269 I geschützt werden, ist von keiner praktischen Bedeutung. Datenträger, die Daten für den Menschen unmittelbar wahrnehmbar speichern — Lochkarten und Lochstreifen — werden wegen der technischen Entwicklung in Zukunft kaum noch benutzt werden. Soweit Schriftstücke mit Hilfe von Scannern verarbeitet werden, werden sie durch § 267 I ausreichend geschützt. Die gegenteilige Ansicht läßt sich nicht aus dem Wortlaut, sondern nur durch die Gesetzessystematik und durch die Entstehungsgeschichte des § 269 rechtfertigen.[9]

Nach ihrer Funktion oder Bestimmung kann zwischen Eingabe-, Ausgabe-, Stammdaten und Zwischenergebnissen unterschieden werden. Auch die aus Konstanten, Variablen und Funktionen zusammengesetzten Programme stellen selbst Daten dar.[10]

b) Die Beweiserheblichkeit von Daten

Das Merkmal „beweiserheblich" erscheint im Tatbestand des § 269 I zweimal. Zunächst ist „beweiserheblich" ein wesentliches Attribut der Daten. Hinzu kommt die Beweisfunktion durch hypothetischen Vergleich der Daten mit einer Urkunde i.S.v. § 267 I. Im Rahmen des § 267 I umfaßt die Beweisfunktion die Beweiseignung und die Beweisbestimmung (von vornherein durch den Aussteller, oder später, ggf. durch einen Anderen) für eine rechtlich relevante Tatsache.[11] Zum Beweis geeignet ist eine Urkunde, wenn sie für sich, oder i.V.m. anderen Umständen, für die Überzeugungsbildung mitbestimmend ins Gewicht fallen kann.[12] Davon zu unterscheiden ist die Beweiskraft. Sie bemißt sich nach anderen Kriterien (z.B. §§ 415–419 ZPO) und spielt hier keine Rolle.

Angesichts der weiten Auslegung durch die Rechtsprechung werden diese Merkmale von der Literatur kritisch betrachtet. Im Rahmen des § 269 kann der Begriff Daten auf rechtliche und wirtschaftliche Daten beschränkt werde. Technische und wissenschaftliche Computernutzung dient in der Regel nicht dem Rechts- und Beweisverkehr. Die hier entstehenden Daten erhalten eine Beweisfunktion nur dann, wenn sie besonders in rechtliche Erklärungen einbezogen werden.[13] Dies gilt ebenso für innerbetriebliche Daten, es sei denn, diese dienen dem innerbetrieblichen Rechts- und Beweisverkehr.[14] Somit kann der Datenbegriff auf rechtliche und wirtschaftliche Daten beschränkt werden.

4. Die Fiktion der Wahrnehmbarkeit von Daten und die „hypothetische"Subsumtion unter § 267

a) Die Methodik des Gesetzgebers und ihre Bedeutung

Der Gesetzgeber schreibt durch die Formulierung **„[...], daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, [...]"**

5. Beschlußempfehlung und Bericht des **Rechtsausschusses (RA-BT)** vom 19. Febr. 1986, **BT-Drucks.** 10/5058 S.33f. Ebenso **Dreher/Tröndle**, Strafgesetzbuch mit Nebengesetzen, 43. Aufl. 1986, § 269 Rn. 1. **Lackner**, Strafgesetzbuch mit Erläuterungen, 17. Aufl. 1987, § 269 Anm. 1. **Möhrenschlager**, Wistra 1986, 128, 134. **Schlüchter**, 96. **Lenckner/Winkelbauer**, CR 1986, 824. Weitergehend noch **Sieber**, Computerkriminalität, 1/297, 1/355-359, 2/20-24. Tagungsberichte der Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität, Hrsg. vom BMJ 1977, Beschlüsse Nr. 10–15, S. 78–90, wiedergegeben bei Sieber, Computerkriminalität 1/361ff. Anderer Auffassung ist **Bühler**, MDR 1987, 448, 453 ohne Begründung.

6. **RA-BT**, BT-Drucks. 10/5058, 34. **Lenckner/Winkelbauer**, CR 1986, 483, 484. **Dreher/Tröndle**, § 269 Rn. 3. **Lackner**, § 269 Anm. 2.

7. **DIN 44 300** Nr. 19. **Schneider** (Hrsg.), Lexikon der Datenverarbeitung, 2. Aufl. 1986, Stichwort „Daten". **Möhrenschlager** Wistra 1986, 128, 134. **Lenckner/Winkelbauer** CR 1986, 483, 484. **Lackner**, § 269 Anm.3a / § 263 Anm. 3a.

8. **Lenckner/Winkelbauer** CR 1986, 483, 484. **Schönke/Schröder/Cramer** § 268 Rn. 11. **Dreher/Tröndle** § 268 Anm. 3. **Leipziger Kommentar/Tröndle** § 268 Rn. 13.

9. Ebenso **Dreher/Tröndle** § 269 Rn. 3. differenziert **Lenckner/Winkelbauer** CR 1986, 824, 825. Andere **Auffassung Systematischer Kommentar/Samson** § 269 Rn. 19. **RA-BT**, BT-Drucks. 10/5058, 34. **Granderath**, DB 1986 Beilage 18, 1, 5. **Lackner** StGB § 269 Anm. 2. **Möhrenschlager** Wistra 1986, 128, 134.

10. Ebenso **Lenckner/Winkelbauer**, CR 1986, 483, 485. **Lackner**, § 269 Anm. 3a / § 263a Anm. 3a.

11. **Dreher/Tröndle**, § 267 Rn. 9. **Lackner**, § 267 Anm. 2d.bb. **Leipziger Kommentar/Tröndle**, § 267 Rn. 50. **Schönke/Schröder/Cramer**, § 267 Rn. 14. **Systematischer Kommentar/Samson**, 3. Auflage Febr. 1987, § 267 Rn.30-32. Jeweils m.w.N.

12. **Dreher/Tröndle**, § 267 Rn. 10. **Lackner**, § 267 Anm. 2d.aa. **Leipziger Kommentar/Tröndle**, § 267 Rn. 59. **Schönke/Schröder/Cramer**, § 267 Rn. 11. **Systematischer Kommentar/Samson**, § 267 Rn. 29. Jeweils m.w.N.

13. **Dreher/Tröndle**, § 268 Rn. 9. **Schönke/Schröder/Cramer**, § 268 Rn. 25

14. **BGHSt** 3, 82, 85; 13, 382, 385, 387; **BGH GA** 1979, 143f; **RGSt** 38, 46ff. **Sieber** Computerkriminalität 1/286.

die Fiktion der Wahrnehmbarkeit der Daten vor. Der Gesetzesanwender hat also unter dieser Bedingung zu prüfen, ob die betreffenden Daten eine unechte oder verfälschte Urkunde darstellen.

Ziel der Gesetzestechnik „Fiktion" ist die Gleichsetzung zweier Tatbestände, welche tatsächlich ungleich sind, um von einer Norm auf die andere zu verweisen. Statt anzuordnen, daß die Rechtsfolgen des Tatbestandes 1 auch für den Tatbestand 2 gelten, wird fingiert, Tatbestand 2 sei ein Fall von Tatbestand 1.[15] Stattdessen wird hier unterstellt, das Tatbestandsmerkmal XY sei gegeben. Werden dann die Tatbestandsmerkmale A, B, C des Tatbestandes § 267 I und die sonstigen Voraussetzungen des Tatbestandes § 269 I erfüllt, treten dessen Rechtsfolgen ein. Der Rechtsanwender hat also über die Fiktion hinaus Feststellungen zu treffen, die gegebenenfalls den Eintritt der Rechtsfolgen bewirken.[16]

Einer Fiktion kommt suggestive Wirkung zu. Jeder Jurist kennt das Problem der „Sachverhaltsverbiegung" durch unzulässige Unterstellungen. Eventuell hat der Gesetzgeber auch nicht alle Folgen seiner Technik bedacht. Daraus folgt zwingend die behutsame und kritische Anwendung traditioneller Definitionen auf eine neue Norm.[17] Einerseits darf nicht unterstellt werden, die betreffenden Daten stellten hypothetisch eine Urkunde dar. Andererseits dürfen die Begriffe aus § 267 I nicht unkritisch in § 269 I verwendet werden.[18] Auch eine Prüfung, ob die betreffenden Daten ausgedruckt tatsächlich eine Urkunde darstellen, liegt außerhalb der Wortbedeutung der „Fiktion". Vor diesem Hintergrund stellt sich die Frage der Tragweite des § 269 I.

b) Die Perpetuierung von Daten

Wesentliches Merkmal einer Urkunde ist, daß sie die perpetuierte Entäußerung eines menschlichen Gedankens beinhaltet, welche durch vorangegangene Bestimmung (Herkommen, Gesetz, Vereinbarung) des Codes (Sprache, Schriftzeichen etc.) auf einen Sachverhalt hinweist.[19]

Wann können Daten — nach Verarbeitung durch technische Hilfsmittel (Registrierung, Reproduzierung, inhaltliche Veränderung) — noch eine menschliche Gedankenerklärung darstellen? Wird die Erklärung ohne inhaltliche Änderung durch ein technisches Hilfsmittel (z.B. Computer mit Textverarbeitungssoftware) nur fixiert oder in der Darstellung verändert, so hat dies keinen Einfluß auf ihre Qualität als Urkunde. Das RG kam zu der Erkenntnis, es komme auf die Art der Herstellung einer Urkunde nicht an.[20] Der Gegensatz besteht in den Fällen, in welchen technische Hilfsmittel menschliches Verhalten unmittelbar oder mittelbar registrieren und fixieren. Das RG entschied, daß die jeweilige Person den Vorgang nicht nur verursacht haben darf, sondern daß diesem Vorgang ein konkreter menschlicher Gedanke zugrunde liegen muß.[21] Es stellt sich die Frage, ob eine technische Aufzeichnung (z.B. die automatische Registrierung und Speicherung eines Wiegevorgangs durch einen Computer) im Rahmen § 269 I an die Stelle der (hypothetischen) Urkunde treten kann. Bisher lehnen die Kommentatoren dies ab. Werden die automatisch registrierten Daten in einen Datensatz für die Verarbeitung im Rechtsverkehr übernommen (z.B. als Daten für Rechnungen, Materialbuchführung etc.) so stellen sie zwar ggf. beweiserhebliche Daten aber keine menschliche Gedankenerklärung dar.[22]

Wird eine menschliche Gedankenerklärung von einem Computer nicht nur registriert, sondern auch inhaltlich bearbeitet, so fragt man sich, ob das Ergebnis einem Menschen als Erklärung zugerechnet werden kann.[23] Es hat sich jedoch herausgestellt, daß für die Urkundenqualität nicht Entstehungszeitpunkt, -weise oder -art einer Gedankenerklärung entscheidend sind, sondern der Zeitpunkt, ab dem die „beweiserheblichen Daten" einer Person als Erklärung zugerechnet werden können.[24]

Gehaltsfall: Aufgrund eines neuen Tarifvertrags will die Firma F alle Gehälter pauschal um 2% erhöhen. In den Personalakten werden die manuell neuberechneten Grundgehälter eingetragen. Da dem T, der nicht zur Führung der Personalakten berechtigt ist, 2% nicht genügen, erhöht er sein Gehalt um 5%.

T hat hier eine Gedankenerklärung, die nach der Geistigkeitstheorie dem Firmeninhaber zuzurechnen ist, in ihrem Inhalt verfälscht. Die Strafbarkeit ergibt sich somit aus § 267 I.

15. Vgl. **Larenz** Methodenlehre der Rechtswissenschaft, Studienausgabe 1983 S. 141 m.w.N.

16. ebenso **Schlüchter** S. 99.

17. **Larenz** Methodenlehre S. 143

18. So wohl im Ansatz **Lackner**, § 269 Anm. 2 und 3b, wenn er die Erfüllung aller Merkmale fordert. Kritisch **Dreher/Tröndle** § 269 Rn. 5.

19. **Systematischer Kommentar/Samson** § 267 Rn. 13-15.

20. „Schreibmaschine" **RGSt** 24, 281ff und 57, 11; „Fernschreiber" **RGSt** 8, 92, 97f; „Morsetelegraph" **RG JW** 1908, 166; „Druckpresse" **RGSt** 17, 103ff und **GA** 48, 439; „Registrierkasse" **RGSt** 55, 107; „Lochzange" **RGSt** 29, 118ff; „Stempelmaschine" **RGSt** 52, 65ff und 64, 97ff. weitere Nachweise bei **Kienapfel**, Urkunden im Strafrecht, 1967 S. 166f, Fn. 553-569.

21. z.B. **RGSt** 64, 281; **RG DR** 1942, 1469.

22. **Lackner**, § 269 Anm.3b. **Leipziger Kommentar/Tröndle**, § 268 Rn. 11 m.w.N. zum alten Recht. **Möhrenschlager**, Wistra 1986, 128, 134. **Systematischer Kommentar/Samson**, § 269 Rn. 11. a.A. wohl **Lenckner/Winkelbauer**, CR 1986, 824, 825 wenn sie darauf abstellen, daß beweiserhebliche Daten solche sind, die nach ihrem Aussagegehalt zum Beweis geeignet sind. Ebenso **Granderath**, DB 1986, Beilage 18, 1, 5.

23. **Sieber** Computerkriminalität S. 1/283.

24. **Sieber**, Computerkriminalität 1/274ff; insbes. 1/276, 281, 282 stützt sich auf **Sellilling**, Fälschung, 76ff; **Schneider**, JurA 1970 S. 255f; **Blei**, JA 1971 S. 656; **Puppe**, Fälschung, 95-97, 98f. Vgl. auch **Sieber** Computerkriminalität zum Kindergeld-Fall Nr. 1 = S. 1/48f.; Lieferantenrechnungs-Fall Nr. 7 = S. 1/66ff.; Baurechnungs-Fall Nr. 9 = S. 1/73ff. und Rentenmanipulations-Fall Nr. 28 = S. 1/137f.; sowie 1/276; und Anm. zu **OLG München**, JZ 1977, 408, 412. **Leipziger Kommentar/Tröndle**, § 268 Rn. 22. **Dreher/Tröndle**, § 267 Rn.3. **Lackner**, § 267 Anm. 2a.aa.

Variante 1: Die Personalakten werden mit Hilfe eines Computers verwaltet, während die Berechnung der Gehaltserhöhung manuell erfolgt. T ändert in „seinem" Datensatz das Gehalt um 5%.

§ 267 I greift mangels visuell perpetuierter Gedankenerklärung nicht ein. Die Daten des Datensatzes sind beweiserheblich i.S.v. § 269 I. Die Erklärung über die Gehaltshöhe kann weiterhin dem Geschäftsinhaber zugerechnet werden. Somit könnte § 269 I an die Stelle von § 267 I treten, wie es der Gesetzgeber vorsah.

Variante 2: Die Berechnung der neuen Grundgehälter erfolgt nicht mehr manuell. Stattdessen berechnet ein Programm alle Gehälter neu und trägt die Ergebnisse selbstständig in die betreffenden Datensätze ein.

In diesem Fall beruht die Angabe zur Gehaltshöhe auf einer Berechnung des Computers. Da das Ergebnis demnach keine „menschliche" Gedankenerklärung i.S.v. § 267 I darstellt und sich der Geschäftsherr frühestens mit dem Ausdruck der Gehaltsabrechnung zu dem Ergebnis als Garant bekennt, verfälscht T keine Gedankenerklärung. Hier zeigt sich, daß die Zuordnung „beweiserhebliche Daten" — „menschliche Gedankenerklärung" eigentlich unter dem Merkmal der Ausstellerauthentizität (Garantiefunktion) zu behandeln ist.[25] Läßt man jedoch, wie die an traditionellen Begriffen orientierten Kommentatoren **Lackner** und **Samson**,[26] als beweiserhebliche Daten nur Gedankenerklärungen i.S.v. § 267 I zu, widerspricht dieses der Intention des 2.WiKG, den Tatbestand an Hand der Ausstellerauthentizität einzuschränken (unten 4.d). Aus diesem Grund ist es sinnvoll den Begriff der „menschlichen Gedankenerklärung" aus § 267 I betreffend § 269 I so aufzulösen, daß dieses Merkmal „beweiserhebliche Daten" umfaßt, die dazu bestimmt und geeignet sind in einer Datenverarbeitung für den Rechtsverkehr verarbeitet zu werden.[27] D.h. konkret, die Erklärungsherrschaft[28] des Ausstellers wird ersetzt durch die Herrschaft des Ausstellers über die Verwendung der Daten.

Die beweiserheblichen Daten müssen zumindest für gewisse Dauer auf einem Massenspeicher (Magnetband, -platte, Diskette) fixiert (gesichert) werden. Die zeitweilige Existenz der Daten im Hauptspeicher und nur während des Programmlaufs genügt nicht.[29] In diesem Fall sind die Daten nur durch einen sich ständig wiederholenden Refresh-Algorithmus gesichert. Die „Perpetuierungsfunktion" des § 269 I wird immer dann gegeben sein, wenn beweiserhebliche Daten, die zur Verarbeitung im Rechts- und Beweisverkehr geeignet und bestimmt sind, zum Zweck der Sicherung auf einem Massenspeicher über die Dauer des Programmlaufs hinaus gespeichert werden. Sind die sonstigen Tatbestandsmerkmale erfüllt, hat sich T gem. § 269 I strafbar gemacht.

c) Die Beweiserheblichkeit von Daten

Ein Problem der Subsumtion stellt die Beweisfunktion in der „gesetzlichen Fiktion" dar. **Lackner** versteht unter beweiserheblichen Daten nur diejenigen, die nach ihrem Informationsgehalt Gedankenerklärungen darstellen.[30] Das ist eine problematische Definition, da sich weder durch das Element „Beweiserheblichkeit" das Merkmal „Gedankenerklärung" definieren läßt, noch umgekehrt die Beweiserheblichkeit durch den Begriff der Gedankenerklärung. Wie oben (4.b) gezeigt wurde, kann den zu § 267 I entwickelte Begriff der „menschlichen" Gedankenerklärung bei § 269 I nicht ohne Modifikation sinnvoll verwendet werden. Die Meinung von **Lackner** führt dann zu den „systematischen Brüchen", wie es **Samson** formulierte.[31] Muß ein Begebungsakt des Ausstellers positiv festgestellt werden, sei es im Rahmen der Perpetuierungsfunktion,[32] sei es im Rahmen der Beweisfunktion, so wird beweiserheblichen Daten selten die Qualität von „hypothetischen" Urkunden zukommen.[33] Kann kein Begebungsakt festgestellt werden, wird den Entwürfen pauschal die Urkundenqualität abgesprochen.[34] In Folge wären Daten nur als Entwürfe zu behandeln, da ihnen die Beweisbestimmung fehlt.

Sinnvoll erscheint mir, auf beweiserhebliche Daten (3.b) die allgemeinen Grundsätze zur Beweiseignung des § 267 I anzuwenden.[35] Das bedeutet: Sind Daten zum Beweis einer rechtlich erheblichen Tatsache geeignet, kann die Beweisbestimmung von vornherein durch den Aussteller, oder später durch eine andere Person erfolgen. Die Beweisbestimmung kann durch eine Bestimmung zur Verwendung der Daten im Rechts-und Beweisverkehrs ersetzt werden. Man könnte auch die endgültige Archivierung eines Datensatzes nach seiner Erstellung als Begebungsakt i.S. der h.M. verstehen (4.c). Es ist ebenfalls möglich, im Rahmen dieser Beweisbestimmung neben „hypothetischen" Absichts- auch „hypothetische" Zufalls- bzw. deliktische Urkunden zuzulassen.[36] Zwischenergebnissen des Verarbeitungsprozesses fehlt die Beweisbestimmung und -eignung. Sie werden daher nicht durch § 269 I geschützt.

25. Ebenso **Sieber**, Computerkriminalität, 1/282

26. **Lackner**, § 269 Anm. 3b. **Systematischer Kommentar/Samson**, § 269 Rn. 11. **Haft**, DSWR 1986, 255, 257.

27. **RA-BT**, BT-Drucks. 10/5058 S. 33, 34. So auch **Möhrenschlager**, Wistra 1986, 128, 134. **Lenckner/Winkelbauer**, CR 1986, 824, 825. **Dreher/Tröndle** § 269 Rn. 3.

28. **Leipziger Kommentar/Tröndle**, § 267 Rn. 14. **Puppe**, Urkundenfälschung, JURA 1979, 630, 636.

29. **Lenckner/Winkelbauer**, CR 1986, 824, 825.

30. **Lackner**, § 269 Anm. 3b.

31. **Systematischer Kommentar/Samson** § 269 Rn. 17.

32. **Leipziger Kommentar/Tröndle**, § 267 Rn. 12, 13b, 14.

33. **Schlüchter** S. 102.

34. **BGHSt** 3, 82, 85. **RGSt** 64, 136, 137; 61, 161, 162; 57, 310, 311. **OLG Bremen** NJW 1962, 1455. **Schönke/Schröder/Cramer** § 267 Rn. 14.

35. ebenso wohl **Systematischer Kommentar/Samson** § 269 Rn. 20, 21. **Dreher/Tröndle** § 269 Rn. 3

36. ebenso **Systematischer Kommentar/Samson**, § 269 Rn. 20-24. Kritisch zu den Begriffen **Kienapfel**, Urkunden und andere Gewährschaftsträger, 1979, 67ff, 79f.

d) Die Garantiefunktion

Im Rahmen des § 267 I muß die Urkunde einen Aussteller als Garanten für den Erklärungsinhalt erkennen lassen.[37] Es genügt, wenn sich der Aussteller aus den Umständen (z.B. Briefkopf, Formulargestaltung) ergibt. Läßt sich der Aussteller jedoch erst mit weiterer Beweisführung (z.B. Gutachten über die Handschrift oder Fingerabdrücke) ermitteln, ist er ggf. nicht mehr i.S.v. § 267 I erkennbar. Überträgt man diese Grundsätze auf § 269 I, so muß sich der Aussteller aus den Datensätzen selbst oder aus den Umständen ergeben.

Samson verlangt, daß die betreffenden Umstände mit den Daten „körperlich fest verbunden" sind. Während in der Datenfernverarbeitung i.d.R. Identifikationsschlüssel, Paßwörter etc. mit übersendet werden, stellen Datenträger wie Bänder und Disketten ein Problem dar. Sie lassen nicht immer den geistigen Urheber aus einer äußeren Kennzeichnung des Datenträgers erkennen. Außerdem stellt sich das Problem, daß bei der großen Speicherkapazität dieser Medien i.d.R. auch eine Vielzahl von Ausstellern ergeben kann. Ähnliches gilt für fest installierte Datenträger (z.B. Magnetplattenspeicher). In der Regel werden Eigentümer, Betreiber, der für das Programm Verantwortliche, der über die Daten Verfügungsberechtigte oder der für die Datenerfassung Verantwortliche nicht identisch sein. Es bietet sich an, den Aussteller über EDV-typische Umstände wie Zugangsberechtigungsschlüssel, Paßwörter oder andere Sicherungssysteme in Anwendungssoftware, Betriebssystemen und Hardware festzustellen. Zur Sicherung von Datenbeständen verwendet man u.a. die Zwangsprotokollierung aller Benutzer einer Datenbank und die von ihnen während des Programmlaufs eingegebenen Daten (einschl. der verwendeten Programmbefehle). Auf diese Feststellungen könnte die Geistigkeitstheorie angewendet werden.[38] In diesen Fällen ergibt sich der Aussteller jedoch nur aus „externen" Beweisen, nicht jedoch aus der „hypothetischen" Urkunde selbst. Ergibt sich der Aussteller z.B. nur mit Hilfe von Augenscheinsbeweisen (z.B. Gutachten über Handschrift oder Fingerabdrücke) wird eine Ausstellererkennbarkeit mit der Begründung abgelehnt, daß sich der Betreffende nicht als Aussteller zu dem Inhalt bekennen will.[39] In der EDV muß aus fehlender expliziter Ausstellererkennbarkeit jedoch nicht fehlender Bekenntniswille folgen. Nach der RG-Entscheidung 46, 297 (299) genügt es, wenn äußere Formen (für die Urkunde) gewählt werden, die — nach der Verkehrsauffassung — einem bestimmten Aussteller zugerechnet werden kann. Sollte ein Angestellter einer Firma z.B. falsche Daten speichern, so hängt die Strafbarkeit seines Handelns von dem Umstand ab, ob er zur Speicherung der betreffenden Daten befugt ist. Ist er es, so gilt als Aussteller der Geschäftsherr und es werden straflos falsche Daten gespeichert. Ist er es nicht, so täuscht der Täter über die Identität des Ausstellers und handelt strafbar i. S. § 269 I.[40] Man muß also die EDV-typischen Gegebenheiten und die Organisation der DV in denAnsatz zur Problemlösung einbeziehen (vgl. unten 6).[41]

5. Die möglichen Tathandlungen des § 269

Kabeltrommel-Fall[42]: Die Täter A und B kamen überein, daß der eine von ihnen (A) bei der Firma X große Mengen von Kabeltrommeln beziehen sollte, um sie anderweitig zu verkaufen. Diese Warenlieferungen sollten nicht oder nur zum Teil bezahlt werden. B sollte als Leiter der EDV-Abteilung der Firma X dafür sorgen, daß die nicht bezahlten Warenlieferungen durch Manipulationen in der EDV von X als bezahlt ausgewiesen wurden.

Aufgrund des gemeinsamen Tatentschlusses gründete A zwei Unternehmen, welche die Kabeltrommeln von X beziehen sollten. Um eine sofortige Belieferung zu ermöglichen und Nachforschungen über die Bonität der Firmen zu vermeiden versah B diese Firmen mit Kundennummern, die sie als bekannte Abnehmer auswiesen. Wie erwartet wurden seitens X keine besonderen Nachforschungen eingeleitet. B hatte als Leiter der EDV-Abteilung Einfluß auf die Debitorenbuchhaltung, da die Kontrolle der Debitoren nur über von ihm gefertigte Offene-Posten-Listen erfolgte. B war auch für den Zahlungseingang im Debitorenbereich zuständig (Buchung aller Zahlungseingänge etc.).

Aufgrund des gemeinsamen Tatplanes bezog A über den Zeitraum von 7 Jahren Kabeltrommeln im Wert von ca. 4,5 Mio. DM. Dafür wurden jedoch nur ca. 250.000 DM bezahlt. Die Manipulationen in der EDV-Abteilung der Firma X vollzogen sich nach folgendem Schema:

B sorgte zunächst für die Löschung der offenen Posten betreffend der Lieferungen an A. Mit der Löschung wurde zu Dokumentationszwecken eine Pseudozahlung in Höhe des richtigen Betrages auf das Debitorenkonto verbucht. Somit erschienen die Forderungen von X an A als erfüllt. Harmonisierend und im Gegengewicht zu den gelöschten offenen Posten wurde durch B der Bruttoumsatz pauschal vermindert. Die Nettoumsätze wurden nicht verändert. In Folge dieses Vorgehens wirkte die Buchhaltung abgestimmt, und es gab keine auffälligen Sonderbuchungen.

37. h.M. vgl. **Systematischer Kommentar/Samson** § 267 Rn. 33 m.w.N.

38. **Dreher/Tröndle** § 269 Rn. 5. **Möhrenschlager** Wistra 1986, 128, 135.

39. Vgl. **RGSt** 40, 217, 218; 67, 419, 420. **Kienapfel** Urkunden 1967, 268.

40. Vgl. **Lenckner/Winkelbauer**, CR 1986, 824, 825f. **Winkelbauer**, CR 1985, 40, 42. Darauf begründend die Kritik Tröndles an der Tatbestandsgestaltung, **Dreher/Tröndle** § 269 Rn. 5.

41. vgl. auch **Leipziger Kommentar/Tröndle** § 267 Rn 32.

42. Nach **Zimmerli/Liebl** S. 45ff. **Möhrenschlager**, Die Polizei 1987, 44, 45. **Staatsanwaltschaft Stuttgart** 164 Js 443/82.

a) Speicherung von Daten als hypothetisches Herstellen einer unechten Urkunde

Unter Speichern wird die Eingabe von Daten zum Zweck der Verarbeitung und Archivierung (Perpetuierungsfunktion) im Massenspeicher einer EDV-Anlage. Dabei ist Speichern ein einmaliger interaktiver, durch einen Menschen oder durch die EDV selbst gesteuerter Prozeß.[43] Soweit die Auffassung vertreten wird, auch das Aufbewahren von Daten falle unter den Begriff des Speichern[44], so wird verkannt, daß die Aufbewahrung ein vorheriges Speichern voraussetzt. In diesem Fall ist „gespeichert" ein Attribut der Daten. Die Tathandlung des Speicherns entspricht der Herstellung einer unechten Urkunde, da eine Täuschung über die Identität der ausstellenden (speichernden) Person erfolgt.[45]

In dem Kabeltrommel-Fall stellen die Daten der Buchhaltung (sowohl die der Offene-Posten-Liste, wie die des Debitorenkontos) beweiserhebliche Daten für den innerbetrieblichen wie den außerbetrieblichen Rechtsverkehr dar. Die Speicherung einer Pseudozahlung auf das Debitorenkonto könnte daher eine nach § 269 I 1. Alt. strafbare Tathandlung darstellen. Soweit den Kundennummern eine Beweiseignung zukommt, könnte auch in der Speicherung der Kundennummern eine strafbare Handlung vorliegen. Ob der Datenbestand der Firma X einen Aussteller erkenne ließ (Garantiefunktion), geht aus dem mir vorliegenden Sachverhalt nicht hervor. War B als Leiter der EDV-Abteilung nicht nur für die Kontrolle der Debitorenbuchhaltung zuständig, sondern auch für Speicherung und Korrektur der Buchhaltungsdaten, entfällt eine Täuschung über den wahren Aussteller. B hätte sich in diesem Fall nicht wegen Speicherung unechter Daten strafbar gemacht.

b) Veränderung von Daten als hypothetisches Verfälschen einer Urkunde

Die 2. Begehungsalternative „Verändern" entspricht der Verfälschung einer Urkunde. Das bedeutet, daß die veränderten Daten schon als beweiserhebliche Daten i.S.v. § 269 gespeichert sind, und alle weiteren Merkmale i.S.v. § 269 I gegeben sind. Auf die Art und Weise der Veränderung kommt es nicht an. Wichtig ist nur, daß sich die informationstechnische Bedeutung (d.h. auch der Inhalt) der Daten und somit die Beweisrichtung ändert.[46] Zum Teil wird auch die Löschung oder „Neuadressierung" unter den Begriff des Veränderns subsumiert.[47] Hier wird nicht erkannt, daß der Täter Daten dem Rechtsverkehr entziehen will. Dies entspricht jedoch der Unterdrückung einer Urkunde und nicht der Verfälschung. Solche Tathandlungen werden durch § 274 I Nr. 2 erfaßt.

Sofern dem Bruttoumsatz als Summe aller Umsatzposten innerbetrieblich oder außerbetrieblich eine Beweiseignung und -bestimmung zukommt, könnte B tatbestandlich i.S.v. § 269 I 2. Alt. gehandelt haben. Dies setzt jedoch voraus, daß B nach endgültiger Berechnung und Speicherung einer Buchung die Verfügungsbefugnis über diese Daten verlor, d.h. eine Korrektur der Buchhaltung nur über Sonderbuchungen gestattet wäre. Nur in diesem Fall hätte B sich nach § 269 I strafbar gemacht. Die Löschung von Daten der Offene-Posten-Liste fällt nur dann unter § 269 I, wenn man annimmt, daß § 269 I auch den Gesamtbestand einer Datei (Gesamturkunde) schützt. Andernfalls ist § 274 I Nr. 2 einschlägig.

c) Der Gebrauch von unechten oder verfälschten Daten

Die 3. Begehungsalternative setzt tatbestandlich — i.S. der 1. oder 2. Begehungsalternative — gespeicherte oder veränderte Daten voraus. Interpretiert man „Gebrauchen" wie in § 269 I, so ist diese Alternative bereits erfüllt, wenn die Daten dem zu Täuschenden in irgendeiner Weise zugänglich gemacht werden. Der Gebrauch kann auch durch die Verarbeitung der Daten für den Rechtsverkehr in einer DVA erfolgen.[48] Soweit B strafbar unechte Daten speicherte oder Daten veränderte, wird er sie auch i.S. der 3. Alt. gebraucht haben.

6. Die weiteren Strafbarkeitsvoraussetzungen

Der subjektive Tatbestand setzt vorsätzliches Handeln und die Absicht zur Täuschung im Rechtsverkehr voraus. Durch § 270 steht die „fälschliche" Beeinflussung einer DVA der Täuschung im Rechtsverkehr gleich. Ziel dieser Regelung ist, auch jene Fälle in den Geltungsbereich der Computerdelikte einzubeziehen, in denen Menschen nicht unmittelbar getäuscht werden. Da sich § 269 auf die Identitätstäuschung bezieht, muß die Beeinflussung der DVA eine täuschungsgleiche Handlung sein. Es könnte zum Beispiel die Verwendung eines falschen Identifikationsschlüssels einschließlich des Paßwortes unter diesen Begriff subsumiert werden.[49] Zu dem Verhältnis der Tathandlungen des § 269 untereinander, wie von § 269 zu anderen Tatbeständen werden im allgemeinen die selben Meinungen vertreten, wie für die Konkurrenzproblematik von § 267.[50]

43. **Simitis/Dammann/Mallmann/Reh**, Kommentar zum Bundesdatenschutzgesetz, 3. Auflage 1981. **Lackner**, § 269 Anm. 4a. **Möhrenschlager**, Wistra 1986, 128, 135. **Systematischer Kommentar/Samson** § 269 Rn. 30.

44. **Dreher/Tröndle** § 269 Rn. 5. **Schlüchter** S. 98.

45. **Dreher/Tröndle** § 269 Rn. 5. **Lackner**, § 269 Anm. 4a. **Systematischer Kommentar/Samson** § 269 Rn. 29. **Schlüchter** S. 99.

46. **Dreher/Tröndle** § 269 Rn. 5. **Lenckner/Winkelbauer** CR 1986, 824, 826. **Systematischer Kommentar/Samson** § 269 Rn. 31. **Schlüchter** S. 98. **Möhrenschlager** Wistra 1986, 128, 135. a.A. **Lackner** § 269 Anm. 4b.

47. **Möhrenschlager** Wistra 1986, 128, 135. **Bühler** MDR 1987, 448, 454. Kritisch **Systematischer Kommentar/Samson** § 269 Rn. 31.

48. **Möhrenschlager** Wistra 1986, 128, 135. **Systematischer Kommentar/Samson** § 269 Rn. 32. **Schlüchter** S. 98. **Lenckner/Winkelbauer**, CR 1986, 824, 826.

49. Vgl. **Dreher/Tröndle** § 270. **Systematischer Kommentar/Samson** § 270 Rn. 2ff.

50. Vgl. nur **Systematischer Kommentar/Samson** § 269 Rn.34/35.

7. Forderungen an die Konzeption von Dokumentationssystemen

Wie sich bei der Untersuchung der Perpetuierungsfunktion und der Garantiefunktion ergeben hat, stellt ein Hauptproblem die Ausstellerauthentizität dar. Insbesondere hat die Rechtsprechung zu § 267 entschieden, daß sich der Garant für den Inhalt einer Urkunde aus dieser selbst oder aus den Umständen, welche mit der Urkunde verbunden sind, ergeben muß. Bei der Programmentwicklung von Dokumentationssystemen wird dieser Umstand zu berücksichtigen sein. Die praktische Datenverarbeitung hat zu Sicherungszwekken gegen Datenmißbrauch und Manipulationen Zwangsprotokollierungsmaßnahmen entwickelt. Solche Maßnahmen sind geeignet die Anforderungen der Garantiefunktion zu erfüllen. Es bieten sich zwei mögliche Realisierungswege an. Sollte die Rechtsprechung das Merkmal der Garantiefunktion sehr eng auslegen, muß für jeden einzelnen Datensatz eine Protokollierung erfolgen und in direkten Zusammenhang mit dem Datensatz gespeichert werden. Diese Lösung wäre technisch aufwendig (variable Datensatzlängen) und wirtschaftlich nicht vertretbar. Bei einer großzügigeren Auslegung der Garantiefunktion könnte schon genügen, daß eine Zwangsprotokollierung in dem Dokumentationssystem implementiert wird und ihre Ergebnisse (für das ganze System) seriell in einer Datei gesichert werden.

Darüber hinaus ist organisatorisch dafür Sorge zu tragen, daß Buchungshaltung, Kontrolle, Korrektur und Revision funktionell und personell getrennt werden. Insbesondere sollten die für die abteilungsinterne Kontrolle und Leitung, sowie für die Revision verantwortlichen Personen nicht zur Speicherung oder Änderung von Daten berechtigt sein.

8. Literaturhinweise

Achenbach, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, NJW 1986, 1835ff. **Betzl**, Computerkriminalität — Dichtung und Wahrheit, DSWR 1972, 317ff; Computerkriminalität — Viel Lärm um Nichts, DSWR 1972, 475ff; Die Sicherung des Rechnungswesens, 1974. **Bschorr**, Computerkriminalität, 1987. **Bühler**, Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität MDR 1987, 448ff. **Bunge**, Die größte Gefahr ist der ungetreue Mitarbeiter, Kriminalistik 1987, 75f. **Eck**, Strafrechtliche Probleme der neuen Datendienste der Deutschen Bundespost, Archiv PF 1986, 38ff; Die Neuen Straftatbestände zur Bekämpfung der Computerkriminalität und ihre Bedeutung für die Datendienste der Deutschen Bundespost, Archiv PF 1987, 105ff. **Engelhard**, Computerkriminalität und deren Bekämpfung durch strafrechtliche Reformen, DVR 1985, 165ff. **Geßler**, 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität verabschiedet, Der Kriminalist 1986, 221ff. **Granderath**, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, DB 1986 Beilage 18, 1ff. **Haft**, Zur strafrechtlichen Problematik des Computerbetruges DSWR 1979, 44ff; Computerkriminalität und Datenschutz DSWR 1979, 136ff; Das neue Computerstrafrecht, DSWR 1986, 255ff; Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) Teil 2: Computerdelikte, NStZ 1987, 6ff. **Jaburek/Schmölzer**, Computer-Kriminalität, 1985. **Lampe**, Die strafrechtliche Behandlung der sog. Computer-Kriminalität GA 1975, 1ff. **Lenckner**, Computerkriminalität und Vermögensdelikte, 1981. **Lenckner/Winkelbauer**, Computerkriminalität — Möglichkeiten und Grenzen des 2.WiKG, CR 1986, (I) 483ff, (II) 654ff, (III) 824ff. **Liebl/Grosch**, Datendiebstahl als Form der Computerkriminalität, CR 1985, 162ff. **Marx**, Erfaßt das geltende Strafrecht strafwürdige Handlungen aus dem Bereich der sog. Computerkriminalität? Kriminalpolitische Lehren aus einem Beschluß des OLG München vom 26.7.76, DSWR 1977, 323ff. **Möhrenschlager**, Der Regierungsentwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Wistra 1982, 201ff; Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität — Entstehungsgeschichte und Überblick, Wistra 1986, 123ff; Das neue Computerstrafrecht Wistra 1986, 128ff; Reform des Computerstrafrechts, Die Polizei 1987, 44ff. **Mohr**, Polizeiliches Lagebild der Computerkriminalität, Die Polizei 1987, 37ff. **Mühlen, von zur**, Computer-Kriminalität, Gefahren und Abwehrmaßnahmen 1973 S. 45ff. **OECD-ICCP** No. 10, Computer Related Crime: Analysis of Legal Policy, Paris 1986. **Otto**, Bankentätigkeit und Strafrecht, 1983. **Paul**, Ermittlungsmöglichkeiten und -probleme beim Einsatz von EDV und moderner Bürokommunikation, Die Polizei 1987, 50ff. **Poerting/Pott**, Computerkriminalität, Ausmaß Bedrohungspotential Abwehrmöglichkeiten, 1986. **Rohner** Computerkriminalität. Strafrechtliche Probleme bei „Zeitdiebstahl" und Manipulationen, Diss. Zürich 1976. **Schlüchter**, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, Kommentar mit einer kriminologischen Einführung, 1987. **Sieben/Von zur Mühlen**, Computerkriminalität — nicht Dichtung sondern Wahrheit, DSWR 1972,397ff. **Sieber**, Computerkriminalität und Strafrecht, 1977, 2. Aufl. mit einem Nachtrag, 1980; Informationstechnologie und Strafrechtsreform, 1985; The International Handbook on Computer Crime, 1986. **Sieg**, Strafrechtlicher Schutz gegen Computerkriminalität, JURA 1986, 352ff. **Steinke**, Die Kriminalität durch Beeinflussung von Rechnerabläufen, NJW 1975, 1867ff; Kriminalität durch Beeinflussung von Rechnerabläufen, NStZ 1984, 295; Verbrecher am Rechner, Kriminalistik 1987, 73f. **Tiedemann**, Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber, JZ 1986, 865ff. **Uepping**, Computermißbrauch ... aus der Sicht der Informatik, DVR 1985, 323ff. **Winkelbauer**, Computerkriminalität und Strafrecht, CR 1985, 40ff. **Zimmerli**, Computerkriminalität. Tat, Täter, Aufklärung, Kriminalistik 1987, (I) 247ff, (II) 333ff, (III) 398ff. **Zimmerli/Liebl** (Hrsg.), Computerkriminalität, Computersicherheit, 1984.