## II. Rezension

*Tilman Hoppe**)

# Anscheinsbeweis bei Ausspähen der PIN

Zugleich eine Besprechung zu LG Berlin, Urt. v. 16. 11. 1998 – 51 S 292/98, ZBB 1999, 85 (in diesem Heft)

*Das Urteil des LG Berlin vom 16. November 1998 – 51 S 292/98, ZBB 1999, 85 (in diesem Heft) scheint sich im Ergebnis gegen eine Mehrheitsfront von Entscheidungen zu stellen, die bei Mißbrauch der EC-/Kreditkarte durch Dritte zugunsten des Geldinstituts unterstellen, daß der Kunde dem Dritten die Kenntnis der Geheimzahl in grob fahrlässiger Weise ermöglicht hat. Für das Landgericht Berlin spielt dabei weniger eine Rolle, inwieweit die Geheimzahl vor Entschlüsselung durch Dritte geschützt ist, sondern ob die Geheimzahl bei der Eingabe von Dritten heimlich ausgespäht werden kann.*

**Inhaltsübersicht**

I. Problemstellung
1. Die mißbräuchliche Nutzung von EC-/Kreditkarten
2. Ansprüche des Kunden gegen die Bank bei Mißbrauch der Karte

II. Der Streit um die kryptografische Sicherheit der Geheimzahl
1. Sicherheit der Geheimzahl vor Erraten
2. Sicherheit der Geheimzahl vor Entschlüsselung

III. Das Ausspähen der Geheimzahl
1. Möglichkeiten des Ausspähens
2. Das Urteil des LG Berlin
3. Kriterien für die Annahme des Ausspähens der Geheimzahl

IV. Zusammenfassung

## I. Problemstellung

Derzeit befinden sich im Bundesgebiet 77 Millionen Kredit-, Scheck- und Bankkarten im Umlauf.[1] Die Karteninhaber nehmen an den Geldausgabeautomaten der Banken unter Zuhilfenahme ihrer persönlichen Geheimzahl, der sogenannten PIN (*personal identification number*), jährlich eine Milliarde Verfügungen vor.[2] Im Handel laden 140 000 EC-Terminals über 40 Millionen Scheckkarteninhaber ein, bargeldlos zu bezahlen.[3] Die Sicherheit der Geheimzahl gegenüber Dritten ist für Banken und Verbraucher von entscheidender Bedeutung.

### 1. Die mißbräuchliche Nutzung von EC-/Kreditkarten

In zweifacher Hinsicht droht Mißbrauch im Umgang mit der EC-/Kreditkarte. Kunden können den Diebstahl und Mißbrauch der Karte durch einen Dritten vortäuschen und so versuchen, sich auf Kosten der Bank zu bereichern.[4] In Einzelfällen haben Kunden darüber hinaus auch versucht, Karten selbst zu manipulieren, etwa indem sie auf einer EC-Karte mit einem Computer die eigene Kontonummer durch eine andere ersetzt haben.[5]

Zum anderen ist der Diebstahl der EC-Karte für Dritte eine attraktive Möglichkeit, zusammen mit der Geheimzahl in kurzer Zeit an Geldautomaten Bargeldbeträge in Höhe von mehreren tausend Mark abheben zu können. Der Dieb kann darauf hoffen, daß ihm sein Opfer möglicherweise Hinweise auf die Geheimzahl gibt, sei es als unverschlüsselte Notiz, die zusammen mit der EC-Karte aufbewahrt wird, sei es in Form der ungeschickten Tarnung in Form einer vierstelligen „Telefonnummer".[6] Täter können aber auch die Herausgabe der Geheimzahl von ihren Opfern erpressen.[7] Unabhängig davon haben Kriminelle bisher keine Mühe gescheut, die für die Barauszahlung so wichtige Geheimzahl selbständig zu ermitteln. Presseberichte haben dabei immer wieder die Sicherheit des PIN-Systems gegen solche Angriffe in Frage gestellt.[8] In Ausnahmefällen stammten die Täter sogar aus dem Bereich des Handels und der Banken.[9] Die polizeiliche Kriminalstatistik von 1997 erfaßt rund 53 000 geldkartenbezogene Betrugsfälle mit einem Gesamtschaden von rund 68 Mio. DM.[10]

*) *LL.M., Wissenschaftlicher Mitarbeiter, Humboldt-Universität zu Berlin*

1) Handelsblatt vom 18. 2. 1998, S. 19: „Kartenzahlungen im Handel steigen sprunghaft".

2) *Aepfelbach/Cimiotti*, Zur Sicherheit des ec-Kartensystems, WM 1998, 1218, 1221.

3) Handelsblatt (Fußn. 1).

4) So die Anklage im Fall AG Oschatz NJW 1996, 2385.

5) Vgl. BayObLGSt 1993, 86 – Computerbetrug nach § 263a StGB.

6) Grobe Fahrlässigkeit bejaht: OLG Frankfurt/M. OLG-Report 1997, 6 – offenes Aufbewahren von EC-Karte und PIN in Hausgemeinschaft; LG Essen WM 1993, 546 – Aufbewahren der EC-Karte über Nacht im Auto; AG Kassel WM 1993, 2110 – Notieren der PIN als Telefonnummer im Adreßbuch getarnt; a. A. LG Karlsruhe WM 1990, 63; *Strube*, Haftungsrisiken der ec-Karte, WM 1998, 1210, 1211, m. w. N.

7) AG Frankfurt/M. CR 1998, 723.

8) Vgl. den Bericht in ARD Ratgeber Technik vom 28. 10. 1995 sowie in ZDF/WISO vom 27. 9. 1995, wonach an Geldautomaten der Citibank zwei Wochen lang mit Visa-Karten unter Eingabe einer beliebigen PIN Geld abgehoben werden konnte. Ähnliche Fälle soll es auch bei EC-Karten gegeben haben; der Bundesbeauftragte für Datenschutz erhielt laut Der Spiegel 50/1997 eine neue EC-Karte mit neuer PIN und konnte mit seiner alten PIN die neue Karte nutzen, Nachweis bei *Strube*, WM 1998, 1210, 1213 Fußn. 36; siehe auch Frankfurter Allgemeine Zeitung vom 26. 11. 1997: „Diskussion um Geheimzahlen geht weiter"; Handelsblatt vom 22. 9. 1998, S. 5: „Gericht: PIN auf EC-Karte nicht sicher"; Handelsblatt vom 28. 7. 1998, S. 23: „Wieder Zweifel an der Sicherheit der EC-Karte".

9) Vgl. Handelsblatt vom 14. 9. 1998, S. 45, unter Verweis auf OLG Hamm NJW-RR 1998, 561 = JurPC Web-Dok. 123/1998: EC-Karte und PIN – Mithaftung der Bank für untreue Angestellte; *Pausch*, Die Sicherheit von Magnetstreifenkarten im automatisierten Zahlungsverkehr, CR 1997, 174, 178: Angestellter einer Tankstelle manipuliert das POS-Terminal und ermittelt so die PIN der Kunden.

10) BKA-Statistik 1997, S. 186.

In diesem Spannungsfeld einer doppelten Mißbrauchsmöglichkeit bewegt sich die rechtliche Behandlung von Schadensfällen mit EC-Karten. Auf der einen Seite soll der Kunde einen Mißbrauch durch Dritte nicht einfach vortäuschen können und darüber hinaus sorgfältig mit der durch die EC-Karte eingeräumten Verantwortung umgehen. Auf der anderen Seite gibt es Karteninhaber, die mit ihrer Geheimzahl wirklich sorgsam umgehen und deren Konto nach dem Diebstahl der Karte dennoch leergeräumt wird.[11]

## 2. Ansprüche des Kunden gegen die Bank bei Mißbrauch der Karte

Umstritten ist, worauf sich der Kunde berufen kann, um von der Bank Rückgängigmachung einer möglicherweise unberechtigten Buchung verlangen zu können. Zum Teil wird vertreten, daß dem Kunden ein girovertraglicher Erfüllungsanspruch aus §§ 675, 666 Alt. 3 BGB zustehe, wonach der Auftraggeber einen „Erfüllungsanspruch auf richtiges Buchen und Unterlassen falscher Buchungen hat".[12] Bei dieser Betrachtungsweise ist neben dem vertraglichen Erfüllungsanspruch für die Anwendung von § 812 Abs. 1 Satz 1 BGB kein Raum.[13] Alternativ wird vielfach ein Anspruch aus positiver Vertragsverletzung zugrunde gelegt.[14] Problematisch ist hierbei, daß es an einem durch die Fehlbuchung verursachten Schaden des Kunden fehlt. Denn eine möglicherweise unrichtige Buchung mindert rechtlich gesehen das Guthaben des Kunden nicht.[15] Von den Gerichten wird die Entscheidung dieser Frage im Ergebnis meist offengelassen.[16]

Ist dem Kunden die Karte abhanden gekommen und hat ein Dritter damit an einem Geldautomat verfügt, wird die Bank das Konto des Kunden mit dem entsprechenden Geldbetrag belasten. Denn nach §§ 675, 670 BGB, bzw. nach § 783 BGB bei Verfügungen an Automaten anderer Institute, ist die Bank berechtigt, vom Kunden Ersatz ihrer Aufwendungen in Höhe des ausgezahlten Betrages zu verlangen.[17] Sie verrechnet diesen Anspruch im Girokontokorrent und weist die Belastung im Kontostand aus.[18] Dabei stellt die Eingabe der Geheimzahl zusammen mit der Karte eine Weisung gegenüber der Bank auf Auszahlung des Geldbetrages dar, unabhängig davon, ob die Eingabe durch den Kunden oder einen beauftragten Dritten erfolgt. Gegenüber der persönlichen Auszahlung am Schalter besteht lediglich die Besonderheit, daß die Weisung automatisch weiterverarbeitet wird. Verwendet hingegen ein Dritter Geheimzahl und Karte mißbräuchlich, so liegt eine dem Kunden zurechenbare Weisung an die Bank nicht mehr vor.

Die Eingabe der Geheimzahl zusammen mit der Karte spricht zunächst dafür, daß der Berechtigte eine Weisung erteilt hat, denn grundsätzlich kann nur der Kunde über Karte und Geheimzahl verfügen. Die Rechtsprechung nimmt hier zum Teil einen Anscheinsbeweis zugunsten der Bank an.[19] Teilweise wird aber auch von einer bloßen Beweislastverteilung ausgegangen.[20] Im Ergebnis muß der Kunde jedenfalls beweisen, daß ihm die Karte entwendet wurde.[21] Nach der Rechtsprechung kommt ihm hierbei eine Beweiserleichterung zugute. Entsprechend den für die Kaskoversicherung für Autodiebstähle aufgestellten Grundsätzen[22] muß er lediglich einen Sachverhalt vortragen, der den Schluß zuläßt, daß die EC-Karte abhanden gekommen ist. Gelingt ihm ein ausreichend substantiierter Vortrag, so entfällt ein Anspruch der Bank auf Aufwendungsersatz aus § 670 BGB.[23]

Die Bank hat jedoch einen Schadensersatzanspruch aus positiver Vertragsverletzung gegenüber dem Kunden, wenn dieser einem Dritten die Kenntnisnahme von der Geheimzahl ermöglicht hat.

Die Kundenbedingungen für Kreditkarten begrenzen dem Wortlaut nach die Haftung des Karteninhabers bis zur Verlustmeldung auf einen Höchstbetrag von 100 DM: „Für Schäden, die durch mißbräuchliche Verfügungen vor Eingang der Verlustanzeige entstehen, beschränkt sich die Haftung des Karteninhabers auf einen Höchstbetrag von 100 DM je EUROCARD."[24] Das LG Berlin hat, wie auch schon die erste Instanz,[25] die entsprechende Klausel in seiner hier besprochenen Entscheidung streng dem Wortlaut nach auslegt. Den Einwand der beklagten Sparkasse, daß diese Klausel nach dem Sinn der gesamten Haftungsregelungen nicht für Fälle grob fahrlässigen Verhaltens eingreifen solle, ließ das Gericht nicht gelten, sondern verwies insoweit auf § 5 AGBG, wonach die verbleibende Unklarheit zu Lasten der Beklagten gehe. Mit dieser Entscheidung weicht das LG Berlin von der bisherigen Rechtsprechung ab. Verschiedene Oberlandesgerichte hatten sich in vergleichbaren Fällen auf den Standpunkt gestellt, daß die Haftungsbegrenzung, wenngleich dem Wortlaut nach unbedingt formuliert, nur für solche Sachverhalte Geltung beanspruchen könne, bei denen die Schäden ohne Verschulden des Karteninhabers eingetreten seien.[26] Ausschlaggebend war

11) *Rüßmann*, Haftungsfragen und Risikoverteilung bei ec-Kartenmißbrauch, DuD 1998, 395, 399.

12) So KG WM 1977, 1236, 1237; *Joost*, Die Verteilung des Risikos von Scheckfälschungen, ZHR 153 (1989), 240; *Reiser*, WM 1990, 545 f; *Oechsler*, WuB I D 5c.-4.96; *Canaris*, Bankvertragsrecht, 3. Aufl., 1988, Rz. 527 und 347, stützt den Rückbuchungsanspruch auf die §§ 675, 667 BGB.

13) Grundsätzlich BGH WM 1968, 776; die bereicherungsrechtliche Lösung wird aber vertreten von LG Duisburg WM 1989, 181.

14) So z. B. LG Essen WM 1993, 546; LG Köln WM 1995, 976; AG Hannover WM 1997, 64.

15) *Joost*, ZHR 153 (1989), 240; *Oechsler*, WuB I D 5c.-4.96.

16) Positive Vertragsverletzung oder ungerechtfertigte Bereicherung: OLG Hamm ZIP 1997, 878 = WM 1997, 1203, dazu EWiR 1997, 545 *(Spindler)*; OLG Frankfurt/M. OLG-Report 1998, 6; LG Berlin ZBB 1999, 85, in diesem Heft.

17) *Häde*, Die Zahlung mit Kredit- und Scheckkarten, ZBB 1994, 33, 39.

18) *Rüßmann*, DuD 1998, 395.

19) OLG Frankfurt/M. OLG-Report 1998, 259, 260.

20) OLG Hamm ZIP 1997, 878, 879.

21) OLG Hamm ZIP 1997, 878, 879.

22) BGH NJW 1996, 993.

23) *Rüßmann*, DuD 1998, 395, 396.

24) Nr. 9 EUROCARD-Kundenbedingungen, abgedruckt bei *Gößmann*, in: Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Handbuch, Bd. I, 1997, Anh. 1 zu §§ 67, 68; eine entsprechende Formulierung findet sich in den VISA-Kundenbedingungen.

25) AG Berlin-Mitte, Urt. v. 13. 5. 1998 – 17 C 53/98.

26) OLG Frankfurt/M. OLG-Report 1997, 6; ebenso KG WM 1992, 729; OLG Zweibrücken ZIP 1990, 1548 = WM 1991, 67, dazu EWiR 1990, 1177 *(Kaiser)*.

für die Gerichte dabei die rechtspolitische Überlegung, daß sich Kunden bei wörtlicher Auslegung der Klausel, „geradezu ermuntert fühlen (müßten), unsorgfältig mit den EC-Medien (gemeint ist hier die EUROCARD) umzugehen, weil Folgen außer der Selbstbeteiligung in Höhe von 100 DM nicht zu befürchten sind."[27] Ob diese durchaus begründete Befürchtung allerdings die Gerichte dazu berechtigt, den klaren Wortlaut der Klausel einschränkend auszulegen, erscheint zweifelhaft.[28] Es hätte den Geldinstituten und Kreditkartenorganisationen auch aufgegeben werden können, ihre Kundenbedingungen entsprechend zu gestalten. Denn mit der jetzigen Formulierung wird dem Kunden suggeriert, auch im Falle grober Fahrlässigkeit große Risiken nicht tragen zu müssen.[29]

Auch die Bedingungen für EC-Karten begrenzen die Haftung des Kunden auf die Zeit bis zur Verlustmeldung.[30] Davor haftet der Kunde jedoch ausdrücklich für eine grob fahrlässig verschuldete Verletzung von Sorgfalts- und Mitwirkungspflichten bezüglich der Aufbewahrung der Karte und der Geheimhaltung der Geheimzahl.[31] Grobe Fahrlässigkeit liegt insbesondere vor, wenn die persönliche Geheimzahl auf der EC-Karte vermerkt oder zusammen mit der EC-Karte verwahrt war (z. B. der Originalbrief, in dem die Geheimzahl dem Karteninhaber mitgeteilt wurde).[32] Die Rechtsprechung hat grobe Fahrlässigkeit beispielsweise angenommen, wenn die EC-Karte in einem nicht abschließbaren Schrank am Arbeitsplatz[33] oder über Nacht im Auto[34] zurückgelassen wurde, oder die Geheimzahl als Telefonnummer getarnt zusammen mit der EC-Karte aufbewahrt wurde.[35]

Die Geldinstitute haben demgemäß nach den Bedingungen für EC- und Kreditkarten mit ihrer Schadensersatzforderung gegen den Kunden nur dann Erfolg, wenn sie beweisen können, daß der Kunde in grob fahrlässiger Weise einem Dritten Kenntnis von der Geheimzahl ermöglicht hat. Die Frage, ob für die Bank der Beweis des ersten Anscheins für die Sicherheit der Geheimzahl streitet, steht im Mittelpunkt einer Vielzahl widerstreitender Entscheidungen.

## II. Der Streit um die kryptografische Sicherheit der Geheimzahl

Auch wenn das Ausspähen der Geheimzahl bei der Eingabe durch den Kunden eine häufige und unberechenbare Gefahr für die Sicherheit der Geheimzahl ist (unten III), haben die Gerichte bisher den Blick im wesentlichen auf die Sicherheit der mathematischen Verschlüsselung der Geheimzahl gerichtet. Ein Dritter hat zwei Möglichkeiten, die Geheimzahl anhand der gestohlenen Karte zu ermitteln. Er kann versuchen, die Geheimzahl durch Ausprobieren zu erraten oder den Code zu knacken, mit dem die Geheimzahl verschlüsselt ist.

### 1. Sicherheit der Geheimzahl vor Erraten

Theoretisch bietet eine vierstellige Geheimzahl, die nicht mit einer „0" beginnt, alle möglichen Kombinationen zwischen 1000 und 9999. Bei einem Limit von zwei zulässigen Fehlversuchen besteht eine Wahrscheinlichkeit von 1:3000, die richtige Geheimzahl zu erraten, was den Gerichten für einen Anscheinsbeweis zugunsten der Geldinstitute überwiegend ausgereicht hat. Tatsächlich traten bei den bis 1998 ausgegebenen Karten manche Zahlen zweiunddreißigmal so oft auf wie andere. Die Liste der häufigsten Geheimzahlen konnte man sogar bei der ARD anfordern.[36] Damit bestand bei 10,5 % aller Kunden ein Risiko von 1:72, daß ein entsprechend versierter Täter die richtige Geheimzahl errät.[37] Zudem befand sich bis 1998 auf der Karte eine Ausgleichszahl (das sogenannte Offset der Karte), die dazu diente, die Karte mit der Geheimzahl nicht nur an Geldautomaten des ausgebenden Kreditinstituts, sondern auch an Automaten anderer Institute im In- und Ausland nutzen zu können.[38] Unter Berücksichtigung des Offsets, das gewisse Rückschlüsse auf die Ziffern der PIN zuließ, konnte ein Täter mit entsprechenden Systemkenntnissen seine Ratechancen nochmals beträchtlich steigern. Mit im Handel erhältlichen Computerprogrammen[39] und Kartenlesegeräten war es möglich, das auf der Karte gespeicherte Offset zu lesen, den Fehlversuchszähler zurückzusetzen, sowie das Ausgabelimit und die Gültigkeitsdauer heraufzusetzen.[40] Der Sachverständige *Schindler* vom Bundesamt für Sicherheit in der Informationstechnik spricht daher von einem „unerfreulichen" Sachverhalt.[41]

Mittlerweile haben die Geldinstitute für Abhilfe gesorgt. Der Fehlbedienungszähler wird nicht mehr bloß auf der Karte, sondern jedenfalls im Inland auch on line in der Autorisierungszentrale mitgeführt.[42] Die Ziffern von 1 bis 9 werden auf die Geheimzahlen gleichmäßig verteilt.[43] Außerdem wird bei on line betriebenen Geldautomaten das Offset auf der Karte

27) OLG Frankfurt/M. OLG-Report 1997, 6, 7.

28) So auch *Pfeiffer*, WuB I D 5b.-1.95, S. 198.

29) *Pfeiffer*, WuB I D 5b.-1.95.

30) Abschnitt III 1.4 ec-Bedingungen (Banken), III 1.5 (Sparkassen), Fassung Januar 1995, abgedruckt bei *Nobbe*, in: Schimansky/Bunte/Lwowski (Fußn. 24), Anh. 5 und 6 zu §§ 60–63.

31) Abschnitt II 7.2, 7.4 ec-Bedingungen (Banken); Abschnitt II 6.2, 6.4 ec-Bedingungen (Sparkassen).

32) Abschnitt III 2.4 ec-Bedingungen Banken und Sparkassen. Zu den einzelnen, im Ergebnis jedoch nicht erheblichen Unterschieden der AGB der Banken und Sparkassen *Rüßmann*, DuD 1998, 395, 396 f.

33) AG Charlottenburg WM 1997, 2082; ähnlich OLG Köln NJW-RR 1996, 619, 620; AG Aachen WM 1993, 291, 292.

34) LG Essen WM 1993, 546, zustimmend *Reiser*, WuB I D 5.-3.93; AG Hamburg, Urt. v. 2. 9. 1997 – 4 C 197/97, Nachweis bei *Strube*, WM 1998, 1210, 1216.

35) OLG Frankfurt/M. OLG-Report 1997, 6; LG Essen WM 1993, 546; AG Kassel WM 1993, 2110; LG Karlsruhe WM 1990, 63; *Strube*, WM 1998, 1210, 1211 m. w. N.

36) ARD Ratgeber Technik vom 20. 4. 1997; *Schindler*, ec-Karten: Wie sicher ist die PIN-Nummer?, NJW-CoR 1997, 283, 285.

37) *Schindler*, NJW-CoR 1997, 283, 285.

38) *Werner*, Anscheinsbeweis und Sicherheit des ec-PIN-Systems im Lichte der neueren Rechtsprechung, WM 1997, 1516, 1518.

39) Das LG Frankfurt/M. CR 1998, 269, hat den Verkauf des einschlägigen Computerprogramms „CARDS" in Kaufhäusern der Kaufhof AG wegen dieser Mißbrauchsgefahr als wettbewerbswidrig untersagt. Ein zu dem Computerprogramm „Windows" gehörendes Arbeitsprogramm namens „Hyper Terminal" leistet jedoch die gleichen Dienste, LG Frankfurt/M. CR 1998, 269, 271.

40) LG Frankfurt/M. CR 1998, 269, 271.

41) *Schindler*, NJW-CoR 1997, 283, 285.

42) *Werner*, WM 1997, 1516, 1518 m. w. N.

43) *Stenger*, Zur Kritik an der Annahme einer Errechenbarkeit einer PIN, CoR 1997, 363, 364.

nicht mehr benötigt und daher seit 1997 von den Geldautomaten überschrieben.[44] Gegenüber einem Erraten dürfte die Geheimzahl daher mittlerweile wieder als sicher gelten.

### 2. Sicherheit der Geheimzahl vor Entschlüsselung

Die Verschlüsselung der Geheimzahl funktioniert wie folgt: Bankleitzahl, Kontonummer und Kartenfolgenummer ergeben eine 64stellige Zahl. Diese wird mit einem bislang 56 Stellen breiten Institutsschlüssel, eine Art Generalschlüssel, im sogenannten DES-Verfahren (DES = „Data Encryption Standard") verschlüsselt. Aus dem Ergebnis werden 4 Stellen für die Geheimzahl ausgewählt. Hieraus wird zusammen mit 4 auf der Karte befindlichen Ziffern die endgültige Geheimzahl gewonnen.[45] Hat der Täter den Institutsschlüssel geknackt, kann er zusammen mit einem im Handel erhältlichen Kartenlesegerät die Geheimzahl einer gestohlenen Karte in Sekundenschnelle ermitteln.[46] Seit 1998 werden von den Kreditinstituten Karten ausgegeben, die mit einem nunmehr 128stelligen Schlüssel im sogenannten Triple-DES-Verfahren codiert sind.[47]

Das bis 1998 verwandte Verfahren mit dem 56stelligen Schlüssel sah sich mit technischem Fortschritt zunehmender Kritik ausgesetzt. Das Verfahren ermöglicht 2 hoch 56 (etwa 72 Billiarden) mögliche Schlüssel. Damit sind maximal ebensoviele Versuche notwendig, um den Institutsschlüssel aus mehreren EC-Karten nebst dazugehöriger bekannter Geheimzahl zu errechnen.[48] In einer Entscheidung aus dem Jahre 1992 hatte das Kammergericht keinen Zweifel an der Sicherheit des PIN-Systems, denn 72 Billiarden Möglichkeiten entspreche beim Ausprobieren der Anzahl von Sekunden, die seit der Entstehung des Universums verstrichen sind: „Angesichts dieser Bemerkung des Sachverständigen verstummt jeder Zweifel."[49]

Durch die rasante Entwicklung in der Halbleitertechnik war die Entscheidung jedoch schnell überholt. Schätzte man 1987 den Zeitaufwand zum Errechnen des Institutsschlüssels noch auf 286 000 Jahre, waren es 1994 noch 1 900 Jahre, heutzutage sollen es 19 Tage sein, inklusive Planung und Bau einer Spezialrechenmaschine einige Monate.[50] In einem im Internet ausgeschriebenen Wettbewerb gelang es tausenden miteinander vernetzten Teilnehmern einen DES-Schlüssel 1997 zunächst in 96 Tagen, dann in 56 Stunden und im Januar 1999 binnen 24 Stunden zu knacken.[51]

Für Aufsehen hatte die umstrittene[52] Entscheidung des OLG Hamm aus dem Jahre 1997 gesorgt, derzufolge es nicht ausgeschlossen werden könne, daß sich ein mehrere hunderttausend Mark teurer Rechner in den Händen einer kriminellen Organisation befinde und somit der Institutsschlüssel nicht mehr sicher sei.[53] Das Gericht verneinte daher einen Anscheinsbeweis zugunsten der Bank und gab der Klage des Kunden statt. Diese Entscheidung mag „Anschubhilfe" geleistet haben für die seit 1998 erfolgende Ausgabe von neuen EC-Karten, deren Geheimzahlen nach dem Triple-DES-Verfahren verschlüsselt sind.[54] Nach derzeitigem Kenntnisstand kann der neue Schlüssel nicht gebrochen werden.[55] Er läßt 2 hoch 128 Möglichkeiten zu, was einer 38stelligen Zahl entspricht, gegenüber der 16stelligen Zahl an Möglichkeiten, die sich aus dem bisherigen DES-Verfahren ergibt.

## III. Das Ausspähen der Geheimzahl-Nummer

Der Sachverständige *Schindler* hat ein bemerkenswertes Argument angeführt, warum es seiner Meinung nach wenig wahrscheinlich ist, daß der Institutsschlüssel geknackt worden ist: Es gebe „einfacherere und preiswertere Methoden", nämlich das Ausspähen der Geheimzahl.[56] Hierbei handele es sich neben dem Notieren der Geheimzahl auf der Karte und der Weitergabe an vermeintliche Vertrauenspersonen um eine der „häufigsten Mißbrauchsursachen", gegen die auch kein neues PIN-Verfahren schütze.[57] Um so mehr erstaunt es, daß diese Mißbrauchsmöglichkeit die Gerichte bisher kaum beschäftigt hat.

### 1. Möglichkeiten des Ausspähens

In der Vergangenheit gelangten spektakuläre Fälle vor die Strafgerichte, in denen Dritte die Geheimzahl von EC-Karten ausgespäht hatten. In einem vom Bundesgerichtshof[58] entschiedenen Fall hatte der Täter mit Hilfe von ihm entwickelter Geräte an einem Geldausgabeautomaten zahlreiche Kontendaten und Geheimnummern für codierte Automatenscheckkarten gesammelt und gespeichert, und die Daten mit Hilfe eines Codiergerätes auf Scheckkarten-Blankette übertragen. Insgesamt konnte er so von fremden Konten 140 000 DM abheben. Die früher noch mögliche Übertragung von Kartendaten auf Scheckkartenrohlinge und Nutzung an Geldausgabeauto-

44) *Niehoff*, DuD 1997, 534; *Aepfelbach/Cimiotti*, WM 1998, 1218, 1219.

45) Darstellung des Verfahrens bei *Pausch*, CR 1997, 174, 178.

46) *Schindler*, NJW-CoR 1997, 283, 285.

47) *Schindler*, Die neuen PIN-Nummern der ec-Karten, NJW-CoR 1998, 223.

48) *Schindler*, NJW-CoR 1997, 283, 284.

49) KG WM 1992, 729, 730.

50) *Werner*, WM 1997, 1516, 1517; *Schindler*, NJW-CoR 1997, 283, 284; *Hortmann*, Wie sicher ist die PIN?, DuD 1997, 532, 533, weist auf eine preiswertere Möglichkeit hin, in 695 Tagen mit einem etwa 2000 US-$ teuren Computer den DES-Schlüssel zu knacken.

51) Heise Verlag online, Meldung vom 19. 1. 1999 (www.heise.de/tp/deutsch/inhalt/te/1771/1.html).

52) Gegen OLG Hamm: AG München WM 1995, 1995; AG Hannover WM 1997, 1207, dazu EWiR 1997, 695 *(Hensen)*; AG Charlottenburg WM 1998, 1124; LG Bonn WM 1995, 575; AG Frankfurt/M. WM 1995, 880; AG Wuppertal WM 1997, 1209; KG WM 1992, 729; OLG Celle EWiR 1985, 469 *(Roeseler)*; OLG Zweibrücken ZIP 1990, 1548 = WM 1991, 67; *Aepfelbach/Cimiotti*, WM 1998, 1218; *Werner*, WM 1997, 1516.

53) OLG Hamm ZIP 1997, 878, 881, zustimmend *Strube*, WM 1998, 1210; *Rüßmann*, DuD 1998, 395; *Pausch*, CR 1997, 174, 179; ebenso AG Oschatz NJW 1996, 2385; AG Buchen VuR 1998, 42; AG Darmstadt WM 1990, 543; AG Wildeshausen WM 1998, 1128, 1130; AG Frankfurt/M. CR 1998, 723 (abweichend von AG Frankfurt/M. WM 1995, 880, dazu EWiR 1995, 763 *(Huff)*); zweifelnd AG Osnabrück WM 1998, 1227; offengelassen von OLG Frankfurt/M. OLG-Report 1998, 259, 262.

54) So *Rüßmann*, DuD 1998, 395, 400; einer solchen Anschubhilfe widersprechen *Aepfelbach/Cimiotti*, WM 1998, 1218, 1219 („lange vorbereitet"); ebenso *Niehoff*, DuD 1997, 534, der von präventivem Austausch spricht. Die Ausgabe der neuen Karten soll jedoch erst im Jahre 1999 beendet sein, *Strube*, WM 1998, 1210, 1213 Fußn. 40.

55) *Schindler*, NJW-CoR 1998, 223, 224; *Rüßmann*, DuD 1998, 395, 400.

56) *Schindler*, NJW-CoR 1998, 223, 225.

57) *Schindler*, NJW-CoR 1998, 223, 225.

58) BGHSt 38, 120 = NJW 1992, 445.

maten ist jedenfalls im Inland nicht mehr möglich. An den Geldautomaten wird die Echtheit der Karte durch das kaum zu fälschende physikalische, sogenannte MM-Merkmal erschwert, das nur vom Geldausgabeautomaten lesbar ist.[59] An vielen ausländischen Geldautomaten wird das Merkmal allerdings nicht abgefragt.[60] Bei Abhebungen an ausländischen Geldautomaten ist daher der Anscheinsbeweis für die Sicherheit des PIN-Systems erschüttert, wenn das Geldinstitut nicht anhand des Geräteprotokolls[61] nachweisen kann, daß das MM-Merkmal gelesen worden ist. Denn es fällt in ihre Sphäre, durch entsprechende Strukturmaßnahmen die Sicherheit der Prüfung zu verbessern.[62]

Kaum auszuschließen sind Manipulationen, wie in einem Fall, der sich in den Niederlanden ereignet hat. Ein Angestellter einer Tankstelle hatte die Leitungen eines POS-Terminals (*Point-of-Sale*) angezapft und so sämtliche Kartendaten einschließlich Geheimzahl in seinem angeschlossenen Computer gespeichert.[63] Solche Fälle sind besonders heimtückisch, da der Inhaber die Karte nicht vermissen wird.

Die einfachste Möglichkeit des Ausspähens ist der unbemerkte Blick „über die Schulter" des Karteninhabers bei der Eingabe der Geheimzahl am Geldausgabeautomat oder insbesondere im Gedränge an einer elektronischen Kasse im Handel. Mit etwas Geschick steht diese Möglichkeit jedermann sofort offen. Professionelle Täter machen sich verfeinerte Techniken zunutze. Sie mieten Wohnungen gegenüber von Geldausgabeautomaten in verkehrsreichen Zonen an und spähen mit Hilfe von Ferngläsern, Teleobjektiven oder installierten Miniaturvideokameras die Geheimzahl bei der Eingabe aus.[64] Daneben läßt sich auch die Tastatur manipulieren. Auf einer zuvor gereinigten Tastaturoberfläche kann z. B. ein geübtes Auge an der Stärke der Hautfettspuren erkennen, in welcher Reihenfolge die Ziffern eingegeben wurden.[65] Ebenso werden spezielle Vorsatztastaturen für Geldautomaten verwandt, die über die Tastatur gelegt die eingegebene Ziffernfolge per Funk an einen Computer übertragen. In der von den Geldinstituten selbst aufgegebenen Richtlinie aus dem Jahre 1996 über die Sicherheit der Geheimzahl heißt es daher: „Die PIN-Tastatur muß gegen das Hinzufügen zusätzlicher Baugruppen geschützt sein."[66]

## 2. Das Urteil des LG Berlin

Was die Frage der Sicherheit der Geheimzahl gegen Ausspähen anbelangt, bewegt sich das Urteil des LG Berlin auf juristischem Neuland. Bisher hatte sich nur eine Entscheidung des LG Frankfurt/M.[67] aus dem Jahre 1995 auf die Möglichkeit des Ausspähens der Geheimzahl gestützt. Der Kläger konnte mittels eines Zeugen nachweisen, daß seine Geheimzahl bei der Eingabe an einem Geldautomaten von einem Dritten möglicherweise ausgespäht und anschließend die Karte gestohlen wurde. Diese Form der Kenntnisnahme habe der Kläger gemäß den Vertragsbedingungen nicht zu vertreten. Eine allgemeine Erwägung findet sich auch in einem Urteil des AG Buchen,[68] das neben kryptografischen Gesichtspunkten die Unsicherheit des PIN-Systems darauf stützt, daß die Geheimzahl z. B. mit Hilfe von Minikameras ausgespäht werden könne und daher generell nicht sicher sei. Während einige Gerichte die Möglichkeit des Ausspähens in Betracht ziehen, sie aber für den konkreten Fall mangels entsprechender Anhaltspunkte ausschließen,[69] wird sie von anderen Gerichten nicht ausdrücklich erwähnt.[70]

Das LG Berlin verweist in seinem Urteil zunächst allgemein auf die mangelnden Abschirmvorrichtungen an den Geldautomaten. Der Klägerin waren die EC- und die Kreditkarte zwar morgens in der U-Bahn auf dem Weg zur Arbeit in Berlin-Mitte gestohlen worden, ohne daß sie am selben Tage einen Bankautomaten benutzt hätte. Das Gericht stellt jedoch darauf ab, daß die Klägerin regelmäßig zur gleichen Zeit eine bestimmte U-Bahn benutzte, den gleichen Weg zur Arbeit ging und dabei wiederholt eine bestimmte Filiale der Beklagten aufsuchte. Das Gericht hält es daher für möglich, daß ein „entsprechend suchender Täter" die Klägerin bis an ihren Wohnort am Stadtrand Berlins verfolgte oder morgens in der U-Bahn zur üblichen Uhrzeit der Klägerin auflauerte, um ihr die Karten mit den ihm schon bekannten Geheimzahlen zu stehlen. Demgemäß hatte das AG Berlin-Mitte in erster Instanz entsprechend ausgeführt: „Selbst wenn die Klägerin nicht an dem Tattag eine Abhebung vorgenommen haben sollte, ist es doch möglich, daß der Täter das Verhalten der Klägerin über einen längeren Zeitraum ausgekundschaftet und nach Ausspähen der Geheimnummern die Klägerin auf ihrem täglichen Weg zur Arbeit bestohlen hat."[71]

Ein Verschulden des Karteninhabers, der nicht „zwingend auf in seiner Nähe befindliche Personen" achte, schließt es inzident aus. In erster Instanz sah auch das AG Berlin-Mitte in einem Ausspähen der Geheimzahl durch den Täter „keine per se grob fahrlässige Pflichtverletzung" des Karteninhabers im Sinne der Vertragsbedingungen.[72]

## 3. Kriterien für die Annahme des Ausspähens der Geheimzahl

Die Entscheidung hat für Karteninhaber und Geldinstitute einschneidende Konsequenzen. In der Mehrzahl der Miß-

59) *Gößmann* (Fußn. 24), § 54 Rz. 4; *Aepfelbach/Cimiotti*, WM 1998, 1218.

60) *Hortmann*, DuD 1997, 532, 533.

61) *Gößmann* (Fußn. 24), § 54 Rz. 4.

62) *Strube*, WM 1998, 1210, 1211, 1214; allgemein *Rüßmann*, DuD 1998, 395, 400.

63) *Pausch*, CR 1997, 174, 178.

64) *Pausch*, CR 1997, 174, 178 f.

65) *Pausch*, CR 1997, 174, 176.

66) „Vereinbarung über die Absicherung der ec-PIN in institutseigenen SB-Anwendungen", Anlage II, C 3, abgedruckt in: WM 1996, 1154, 1156; vgl. auch *Aepfelbach/Cimiotti*, WM 1998, 1218, 1221.

67) LG Frankfurt/M. WM 1996, 953.

68) AG Buchen VuR 1998, 42.

69) AG Wildeshausen WM 1998, 1128, 1130; LG Bonn WM 1995, 575; AG Frankfurt/M. CR 1998, 723.

70) LG Hannover WM 1998, 1223; AG Dinslaken WM 1998, 1226; AG Osnabrück WM 1998, 1227; AG Charlottenburg WM 1998, 1224, 1226; ähnlich *Rüßmann*, DuD 1998, 395, 398.

71) AG Berlin-Mitte, Urt. v. 13. 5. 1998 – 17 C 53/98, S. 8 (bisher unveröff.).

72) AG Berlin-Mitte, Urt. v. 13. 5. 1998 – 17 C 53/98, S. 8.

brauchsfälle wird ein Kunde in gewisser Nähe zu dem Diebstahl eine Verfügung mit seiner Karte vorgenommen haben, so daß ein Ausspähen der Geheimzahl nicht auszuschließen ist. Die generelle Aufgabe des Anscheinsbeweises für die Sicherheit des PIN-Systems allein wegen der abstrakten Möglichkeit des Ausspähens würde aber dem Mißbrauch durch Karteninhaber Tür und Tor öffnen.

Zunächst sind die Banken wie auch die Teilnehmer am POS-Verfahren im Handel gehalten, die Bedingungen bei der Eingabe so zu gestalten, daß ein Ausspähen nicht möglich ist. Besonders der Sichtschutz der Eingabetastaturen im Handel erscheint im Falle unübersichtlichen Gedränges allzu dürftig. Es wäre dringend zu überlegen, ob im Handel die Legitimation des Kunden nicht ausschließlich durch Unterschrift geschehen sollte, wie bisher schon im sogenannten POZ-Verfahren.[73] An Geldautomaten sollte der Sichtschutz verstärkt werden und die Aufklärung durch die Geldinstitute bezüglich der Möglichkeit des Ausspähens dem Ausmaß der tatsächlichen Bedrohung gerecht werden.[74] Insoweit ist die Bank darlegungs- und beweispflichtig, daß Geldautomaten, an denen frühere Verfügungen getätigt wurden, so weit als möglich ausspähsicher gestaltet sind.[75] Über solche Anforderungen könnte den Banken ein Anreiz für die Verbesserung ihrer Geldautomaten gegeben werden.

Auf der anderen Seite wird der Kunde darlegungs- und beweispflichtig dafür sein, daß er sich bei der Eingabe der Geheimzahl bei den für die Ausspähung in Betracht kommenden Verfügungen vorsichtig verhalten hat.[76] Hier wird ihm die oben (I 2) erwähnte Beweiserleichterung zugute kommen. Darüber hinaus kann er sich nur auf die Möglichkeit des Ausspähens berufen, wenn er zuvor mit seiner Karte nebst Geheimzahl Verfügungen getätigt hat und diese in zeitlichem und örtlichem Zusammenhang mit dem Diebstahl stehen. Im Streitfalle ist daher immer festzustellen, wann und wo die letzte Abbuchung getätigt wurde.[77]

Auf einen örtlichen Zusammenhang hat die Entscheidung des LG Berlin abgestellt. Allgemein läßt sich formulieren, daß der Diebstahl sich an einem Ort ereignen muß, der es wahrscheinlich erscheinen läßt, daß zuvor bei einer Verfügung der Täter die Geheimzahl bei der Eingabe an einem (nicht ausspähsicheren) Terminal ausgespäht hat und dem Kunden gefolgt ist. Entsprechendes muß für den zeitlichen Zusammenhang gelten. Hierauf hatte das LG Frankfurt/M. neben dem örtlichen Zusammenhang seine zitierte Entscheidung[78] gegründet. Zu berücksichtigen ist dabei, inwieweit eine Verfolgung des Karteninhabers nach dem Ausspähen der Geheimzahl für den Täter noch wirtschaftlich ist. Dies ist vor dem Hintergrund zu sehen, daß bei den üblichen Schadensfällen vom Täter bis zu über 10 000 DM abgehoben werden.[79] Ist es dem Täter gelungen, die Geheimzahl auszuspähen, so kann es sich für ihn lohnen, den Karteninhaber über eine weitere Entfernung zu verfolgen und ihm auch noch einige Zeit später an einem gewohnten Ort, etwa einer regelmäßig benutzten Filiale des Geldinstituts, aufzulauern, um einen Diebstahl zu versuchen.

Denkbar ist auch, daß ein Täter sich das Aussehen bestimmter Kunden merkt und Listen mit ausgespähten Geheimzahlen führt, um bei passender Gelegenheit in einer Filiale die Verfolgung aufzunehmen und den Diebstahl der Karte zu versuchen. Schon bei einer erfolgreichen Tat pro Woche ist der Aufwand für den Täter mehr als lohnend. Der Sachverhalt, der der Entscheidung des LG Berlin zugrunde lag, bewegt sich daher noch in einem Bereich, in dem ein Ausspähen örtlich und zeitlich plausibel mit dem Diebstahl der Karte in Zusammenhang gebracht werden kann.

## IV. Zusammenfassung

Bei näherer Betrachtung zeigt sich, daß sich das Urteil des LG Berlin nur dem Anschein nach gegen die bisherige Rechtsprechung stellt. Die Möglichkeit des Ausspähens ist bisher nicht grundsätzlich als abwegig verworfen worden, sondern wurde mangels Verfügungen des Klägers mit seiner Geheimzahl oder mangels Anhaltspunkten für die Möglichkeit des Ausspähens außer acht gelassen.[80] Es ist erfreulich, daß das LG Berlin einen Akzent gesetzt hat, der Gerichte und Beteiligte in künftigen Verfahren veranlaßt, die Möglichkeit des Ausspähens der Geheimzahl genau zu prüfen. Es ist zu hoffen, daß diese Entscheidung Anschubhilfe leisten wird, die Identitätskontrolle mit Geheimzahl durch ausspähsichere, biometrische Verfahren zu ersetzen, die den Fingerabdruck des Karteninhabers überprüfen. Solche Verfahren werden schon bei Zugangskontrollen zu Betrieben verwendet und ließen sich kostengünstig durch einen Chip auf der Karte vornehmen.[81]

73) Point-of-Sale ohne Zahlungsgarantie, siehe *Häde*, ZBB 1994, 33, 41.

74) Vgl. *Schindler*, NJW-CoR 1998, 223, 226.

75) *Strube*, WM 1998, 1210, 1211, 1214.

76) *Schindler*, NJW-CoR 1998, 223, 226.

77) Vgl. *Pausch*, CR 1997, 174, 176.

78) LG Frankfurt/M. WM 1996, 953.

79) So etwa im Fall OLG Frankfurt/M. OLG-Report 1997, 6; OLG Frankfurt/M. OLG-Report 1998, 259, 262: Schadenssumme über 20 000 DM.

80) AG Wildeshausen WM 1998, 1128, 1130; LG Bonn WM 1995, 575; AG Frankfurt/M. CR 1998, 723; LG Hannover WM 1998, 1223; AG Dinslaken WM 1998, 1226; AG Osnabrück WM 1998, 1227; AG Charlottenburg WM 1998, 1224, 1226.

81) *Schindler*, NJW-CoR 1998, 223, 226.