Sonderdruck aus Heft 8.2014 // Seiten 389–393

Betriebs Berater

Dr. Michael Fingerhut, RA

Datenmissbrauch und Geheimnisverrat durch Mitarbeiter – die Bedeutung des § 17 UWG

In der Wirtschaft nehmen die Fälle von Geheimnisverrat und Datenmissbrauch dramatisch zu. Das ist eine ernste Entwicklung, weil Unternehmensgeheimnisse im Wirtschaftsleben eine große Rolle spielen. Unternehmen haben nicht nur ein Interesse an der Geheimhaltung von technischem Know-how, sondern auch von vertraulichen Daten ihrer Kundenbeziehungen. Datenmissbrauch und Geheimnisverrat werden zunehmend auch von Mitarbeitern in den betroffenen Firmen begangen, die sich verändern wollen und firmeninterne Daten widerrechtlich „mitnehmen", um sie sich in einer neuen Position zunutze zu machen. Häufig sind sogar die neuen Arbeitgeber an solchen Aktionen beteiligt, um unter Ausnutzung geheimer Daten Wettbewerb zu machen und gezielt Kunden „abzugraben". Betroffene Unternehmen stehen solchen Machenschaften oft deshalb hilflos gegenüber, weil sie sie entweder nicht bemerken oder aber – häufig in Unkenntnis ihrer Rechte – entweder gar nicht, falsch oder zu spät reagieren. Ziel dieses Beitrags ist die Darstellung der den betroffenen Unternehmen zustehenden rechtlichen Möglichkeiten bei Geheimnisverrat und Datenmissbrauch durch Mitarbeiter.

I. Betriebsgeheimnisse im Arbeitsrecht

Auszugehen ist davon, dass Mitarbeiter grundsätzlich berechtigt sind, im Rahmen ihres Dienstverhältnisses erworbene Kenntnisse und Kundenbeziehungen auch nach ihrem Ausscheiden aus einem Unternehmen zu nutzen. Ein Mitarbeiter darf also auch nach seinem Weggang Kunden seines früheren Arbeitgebers ansprechen, denn diese Kundenbeziehungen sind regelmäßig offenkundig, weil ein Interessierter sie ohne besondere Schwierigkeiten und Mühen in Erfahrung bringen kann.[1]

Sind die Kenntnisse allerdings vertraulich, unterliegen sie der vertraglichen Verschwiegenheitspflicht des Arbeitnehmers.[2] Dabei wird überwiegend zwischen Betriebsgeheimnissen für den technischen Betriebsablauf und Geschäftsgeheimnissen für den kaufmännischen Bereich unterschieden.[3]

Die Betriebsgeheimnisse bestehen regelmäßig im schutzrechtlich nicht geschützten Bereich und umfassen insbesondere Know-how und Produktionsanweisungen, die Geschäftsgeheimnisse betreffen alle Kenntnisse über Betriebsabläufe und Kundenbeziehungen. Wesentliches Merkmal von Betriebs- und Geschäftsgeheimnissen ist, dass sie außerbetrieblichen Dritten nicht zugänglich sind.

Know-how und technische Betriebsabläufe werden regelmäßig von der vertraglichen Verschwiegenheitspflicht geschützt, ggf. auch erst durch nachvertragliche Vereinbarungen.[4] Problematisch ist daher in der Regel der Schutz der Geschäftsgeheimnisse, also des kaufmännischen Bereichs.

Wie ausgeführt, darf ein betrieblicher Mitarbeiter nachvertraglich Kunden seines früheren Arbeitgebers mit dem Ziel ansprechen, sie zu einem Geschäftsabschluss mit seinem neuen Arbeitgeber zu veranlassen. Verboten ist ihm jedoch, dass er im Rahmen einer neuen Tätigkeit Kenntnisse insbesondere über

- Kundenlisten und Kalkulationsparameter seines früheren Unternehmens

und

- Kontaktdaten wie Gesprächspartner, Direkttelefone, E-Mail-Adressen des Zielunternehmens

benutzt, die im Laufe seiner Tätigkeit bei seinem früheren Unternehmen aufgebaut/erworben wurden und nicht als offenkundig angesehen werden können. In der Regel hat ein Mitarbeiter diese Daten für seine Tätigkeit auf seinem PC gespeichert.[5] Scheidet er dann aus seinem bisherigen Unternehmen aus und nimmt er die Daten mit, sind diese für seine künftige Arbeit bei einem Wettbewerbsunternehmen von großem Nutzen, ihre Verwendung für das frühere Dienstunternehmen höchst nachteilig.

Ein Unternehmen kann einem solchen Missbrauch seiner Geschäftsgeheimnisse in erster Linie durch ein nachvertragliches Wettbewerbsverbot (§§ 74 ff. HGB) entgegenwirken. Aber Wettbewerbsverbote sind teuer und die Überwachung ihrer Einhaltung oft schwierig, weshalb sie eher selten vereinbart werden.

In Betracht kommt ferner eine im Arbeitsvertrag zu vereinbarende Verschwiegenheitsabrede. Sie ist – wenn sie den Arbeitnehmer in seinem beruflichen Fortkommen einschränkt – als qualifizierte Verschwiegenheitsvereinbarung einem Wettbewerbsverbot gleichzustellen und ohne Entschädigungsregelung unwirksam.[6] Schränkt eine solche Verschwiegenheitsabrede den Mitarbeiter dagegen nicht ein (einfache Verschwiegenheitsvereinbarung), unterliegt sie nach herrschender Meinung zwar nicht den Anforderungen des Wettbewerbsverbots, soll aber wegen Art. 12 GG nur in einer zeitlichen Begrenzung von maximal zwei Jahren wirksam sein.[7]

Vorstehend geschilderte Unterscheidung der Rechtsprechung nach der Einschränkung im beruflichen Fortkommen ist natürlich unscharf und für vorbeugende vertragliche Regelungen wenig hilfreich. Im Ergebnis bleibt somit die Erkenntnis, dass die Rechtsprechung der Arbeitsgerichte dem Unternehmer gegen untreues Verhalten eines Mitarbeiters nach dessen Ausscheiden durch vorbeugende vertragliche Vereinbarungen keinen zuverlässigen Schutz bietet.

1 Vgl. BAG, 26.2.1987 – 6 ABR 46/84, BB 1987, 2448, DB 1987, 2526.
2 Vgl. hierzu grundsätzlich *Küttner*, Personalbuch 2013, Stichwort „Betriebsgeheimnis", Rn. 2.
3 Vgl. *Küttner*, Personalbuch 2013, Stichwort „Betriebsgeheimnis", Rn. 2.
4 Vgl. zur Unterscheidung *Küttner*, Personalbuch 2013, Stichwort „Betriebsgeheimnis", Rn. 7.
5 Verursacht oder gefördert wird dies oft durch die in Unternehmen zunehmend gepflogene Praxis des „Bring your own Device" (BYOD als Betriebsmittelersatz).
6 Vgl. BAG, 15.12.1987 – 3 AZR 474786, DB 1988, 1020.
7 Vgl. z. B. *Küttner*, Personalbuch 2013, Stichwort „Betriebsgeheimnis", Rn. 8.

Gerade deshalb kommt § 17 UWG besondere Bedeutung zu. Der Gesetzgeber hat diese Norm im UWG kodifiziert, weil die Vorschrift auch Datenmissbrauch und Geheimnisverrat durch einen Mitarbeiter ausdrücklich für den Fall unter Strafe stellt, dass diese Handlungen – was die Regel sein dürfte – zu Zwecken des Wettbewerbs erfolgen.

II. Die gesetzliche Regelung in § 17 UWG

1. Allgemeines

Als Strafnorm schützt die Vorschrift den Unternehmer vor einer Verletzung seiner Geschäfts- und Betriebsgeheimnisse. Normadressaten sind die bei einem Unternehmen beschäftigten Personen, aber auch Wettbewerber, die sich von Mitarbeitern unbefugt verschaffte Geheimnisse zunutze machen, indem sie sie selbst verwerten oder weitergeben. Die strafbedrohte Ausgangshandlung ist stets das rechtswidrige Verhalten von Mitarbeitern, die Betriebsgeheimnisse während ihrer Tätigkeit Dritten zuspielen oder danach in eine neue Anstellung mitnehmen und sie im Interesse ihres neuen Arbeitgebers verwerten.

2. Tatbestände des §17 UWG

§ 17 UWG unterscheidet in drei Tatbestände

- den Geheimnisverrat durch einen Mitarbeiter (§ 17 Abs. 1 UWG),
- die Betriebsspionage durch einen Mitarbeiter oder einen sonstigen Dritten (§ 17 Abs. 2 Nr. 1 UWG),
- die Geheimnisverwertung/Geheimnishehlerei[8] durch einen noch tätigen oder ausgeschiedenen Mitarbeiter oder einen Dritten (§ 17 Abs. 2 Nr. 2 UWG).

Zum Begriff des Geschäftsgeheimnisses i.S.d. § 17 UWG nach dem Ausscheiden eines Mitarbeiters hat der BGH in zwei grundlegenden Entscheidungen Stellung genommen und zugunsten des jeweils klagenden Unternehmens ein Geschäftsgeheimnis an mitgenommenen Daten bejaht.[9]

Im Einzelnen:

a) Geheimnisverrat (Abs. 1)

Der Täterkreis des Abs. 1 ist im Interesse eines umfassenden Geheimnisschutzes weit auszulegen; er umfasst alle Beschäftigten eines Unternehmens.[10] Tatobjekt ist ein Geschäfts- oder Betriebsgeheimnis, das dem beim betroffenen Unternehmen Beschäftigten anvertraut oder mitgeteilt wurde.[11] Tathandlung ist die unbefugt – also unter Verstoß gegen eine ausdrücklich auferlegte oder sich konkludent aus dem Vertragsverhältnis ergebende Verschwiegenheitsverpflichtung – erfolgende Mitteilung des Geheimnisses an einen Dritten. Tatzeit ist der Zeitraum der Beschäftigung des Mitarbeiters für den Dienstgeber.

Subjektiv ist erforderlich, dass der Täter vorsätzlich und darüber hinaus mindestens aus einem der folgenden Motive gehandelt hat:

- Zu Zwecken des Wettbewerbs (jeder Art, also eigenen oder fremden, gegenwärtigen oder künftigen Wettbewerb),
- aus Eigennutz (umfasst jede Art von Vorteil),
- zugunsten eines Dritten (jeder Dritte, insbesondere ein künftiger Arbeitgeber),
- in der Absicht, das betroffene Unternehmen zu schädigen (Absicht ist Wollen des Schadens).

In der Praxis ist der Hauptfall die Weitergabe von Betriebsgeheimnissen an einen Wettbewerber gegen Geld oder zur Vorbereitung einer künftigen Tätigkeit für diesen.

b) Betriebsspionage (Abs. 2 Nr. 1)

Der Täterkreis bei der Betriebsspionage des Abs. 2 Nr. 1, umfasst jedermann, auch einen Mitarbeiter des Unternehmens. Der Tathergang ist in Abs. 2 lit. a–c, definiert:

- Die Anwendung technischer Mittel umfasst insbesondere Fotokopierer, Kameras und jede Art von Abhöranlagen, aber auch das „Anzapfen" von EDV-Anlagen und Telefonen[12] und die Verwendung von Computern.[13]
- Die Herstellung einer verkörperten Wiedergabe ist nicht auf die technischen Mittel der lit. a.) beschränkt, sondern umfasst auch Zeichnungen sowie den Nachbau und die spätere Aufzeichnung.[14]
- Die Wegnahme einer Sache bedeutet die Gewahrsamsverschaffung eines Gegenstands, der das Betriebsgeheimnis verkörpert oder enthält. Sie kann durch Wegnahme, d.h. Bruch fremden Gewahrsams, oder Sicherung, d.h. Bewahrung einer schon vorhandenen Kenntnis, erfolgen.

Insbesondere das letztgenannte Tatbestandsmerkmal der Sicherung wirft Fragen auf. So hat der BGH in einem neuen Urteil vom 23.2.2012[15] entschieden, eine Sicherung im Sinne des Abs. 2 Nr. 1 c) 2. Alt., liege nicht vor, wenn ein Beschäftigter bei Beendigung seiner Tätigkeit die Kopie eines geheimen Dokuments mitnehme, das er im Rahmen seiner Tätigkeit befugt angefertigt oder erhalten habe. Eine Wegnahme im Sinne dieser Vorschrift sei nicht gegeben, wenn der Täter befugterweise bereits Alleingewahrsam an der Verkörperung habe.

Diese Entscheidung ist bedenklich. Wenn ein Mitarbeiter im Rahmen einer dienstvertraglichen Tätigkeit Betriebsgeheimnisse – z.B. auf seinem Computer – erwirbt, begründet er keinen Gewahrsam für sich selbst, sondern für das Unternehmen, für das er arbeitet. Das folgt aus der Natur seines Dienstvertrags, aufgrund dessen er nicht für sich, sondern für seinen Dienstherrn tätig ist. Aufgrund dieser BGH-Entscheidung wird man Unternehmen jedoch raten müssen, entweder einen Mitarbeiter an Dienstgeheimnissen keinesfalls Alleingewahrsam begründen zu lassen oder in einer ausdrücklichen Vertragsklausel festzulegen, dass ein Mitarbeiter verpflichtet ist, einen im Rahmen seiner betrieblichen Tätigkeit begründeten Alleingewahrsam bei Vertragsende zugunsten des Dienstherrn aufzugeben.

Für den subjektiven Tatbestand gilt das unter vorstehend unter a.) Gesagte.

c) Geheimnisverwertung (Abs. 2 Nr. 2)

Täter im Sinne der Geheimnisverwertung des Abs. 2 Nr. 2 kann jedermann, also auch ein ausgeschiedener Mitarbeiter, sein. Nach ihrer Zielrichtung erfasst die Norm aber insbesondere Konkurrenzfirmen, die beschaffte oder ihnen überlassene Betriebsgeheimnisse des betroffenen Unternehmens verwerten – das ist jede Art wirtschaftlicher Nutzung – oder jemandem mitteilen – das ist jede Überlassung an einen Dritten.

Beim subjektiven Tatbestand reicht jeder – also auch bedingter – Vorsatz hinsichtlich der Tatbestandsverwirklichung aus. Bei Konkurren-

8 Aus Vereinfachungsgründen wird im Folgenden nur der Begriff der Geheimnisverwertung verwendet.

9 BGH, 27.4.2006 – I ZR 126/03, WRP 2006, 1511, GRUR 2006, 1044 (Kundendatenprogramm); 26.2.2009 – I ZR 28/06, WRP 2009, 613, GRUR 2009, 603 (Versicherungsvertreter).

10 Vgl. hierzu im Einzelnen *Köhler*, in: Köhler/Bornkamm, UWG, 31. Aufl. 2013, Anm. 14 zu § 17

11 Vgl. zum Anvertrauen oder Mitteilen *Köhler*, in: Köhler/Bornkamm, UWG, 31. Aufl. 2013, Anm. 16 und 17.

12 Vgl. LG München I, 23.3.1998 – 6 KLs 315 Js 18225/94, Computerrecht Intern (CI).

13 Vgl. BayObLG, 28.8.1990 – Reg 4 St 250/89, GRUR 1991, 694.

14 Nach BGH, 14.1.1999 – I ZR 2/97, BB 1999, 1452, WRP 1999, 912, ist die bloße Gedächtnisspeicherung nicht ausreichend.

15 BGH, 23.2.2012 – I ZR 136/10, GRUR 2012, 1048, Rn. 14 – Movicol-Zulassungsantrag.

ten, denen ein Mitarbeiter Betriebsgeheimnisse seines früheren Dienstherrn überlässt, muss der Vorsatz also auch das Wissen umfassen, dass dieser sich die Informationen unbefugt verschafft und/oder sie unbefugt „mitgenommen" hat.

Begünstigte Unternehmen lassen sich in der Regel ein, ihnen sei gar nicht bekannt, dass ihr neuer Mitarbeiter bei seiner Tätigkeit Betriebsgeheimnisse seines früheren Dienstgebers nutze und/oder diese sich ihm befugt verschafft habe.

Um diesen Einwand zu entkräften, ist ein sofortiger Hinweis des Geschädigten an das begünstigte Unternehmen erforderlich, dass der ehemalige Mitarbeiter sich das in Frage kommende Betriebsgeheimnis unbefugterweise verschafft oder mitgenommen hat und im neuen Unternehmen deshalb rechtswidrigerweise nutzt – verbunden mit der Aufforderung, diese Nutzung unverzüglich zu unterbinden.[16]

d) Versuchsstrafbarkeit

Von Bedeutung ist schließlich, dass bei allen drei vorgenannten Tatbeständen (a bis c) schon der Versuch strafbar ist, § 17 Abs. 3 UWG.

III. Strafrechtliche Verfolgung

Die vorstehend unter II. beschriebenen Verhaltensweisen sind strafbar; das Strafmaß beträgt Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (§ 17 Abs. 1 UWG), in besonders schweren Fällen Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe (§ 17 Abs. 4 UWG). Die Strafverfolgung setzt jedoch grundsätzlich einen Antrag voraus (§ 17 Abs. 5 UWG). Antragsberechtigt ist nur der Verletzte (§ 77 Abs. 1 StGB). Der Antrag muss innerhalb von drei Monaten ab Kenntniserlangung gestellt werden (§ 77 b StGB).

Betroffenen Unternehmen ist zu raten, sofort nach Kenntniserlangung die Rechtsabteilung oder den Firmenanwalt einzuschalten, damit der Strafantrag rechtzeitig gestellt und bei den Strafverfolgungsbehörden die Ermittlungen angeregt werden. Wichtig ist hierbei eine präzise Zuarbeit des betroffenen Unternehmens bei der Informationserteilung an die Strafverfolgungsbehörden, insbesondere eine ausführliche Beschreibung des Sachverhalts und der Tatumstände. Die Staatsanwaltschaften sind nach dem Amtsermittlungsprinzip verpflichtet, unverzüglich alle erforderlichen Ermittlungen anzustellen, bei den Tatbeteiligten Durchsuchungen durchzuführen und Beweismittel zu beschlagnahmen. Dies ist regelmäßig für die Beweissicherung und die Durchsetzung von zivilrechtlichen Ansprüchen von entscheidender Bedeutung, weil oft nur durch sichergestellte Unterlagen bewiesen werden kann, dass verratene Betriebsgeheimnisse in den Besitz des untreuen Mitarbeiters und/oder eines Konkurrenzunternehmens gekommen sind. Da die volle Beweislast für Geheimnisverrat und Datenmissbrauch nach den allgemeinen zivilrechtlichen Beweisregeln bei den betroffenen Unternehmen liegt und erfahrungsgemäß eine häufig schwierige Hürde bei der Geltendmachung zivilrechtlicher Ansprüche ist, ist die rechtzeitige Einschaltung der Strafverfolgungsbehörden so wichtig.

Selbst wenn die Staatsanwaltschaft ordnungsgemäß ermittelt und die gebotenen Durchsuchungs- und Sicherstellungsmaßnahmen durchführt, neigt sie häufig dazu, das Verfahren mangels öffentlichen Interesses einzustellen und die betroffenen Unternehmen auf den Privatklageweg zu verweisen. Denn das öffentliche Interesse wird in der Regel nur bejaht, wenn der unbestimmte Rechtsbegriff der „volkswirtschaftlich erheblichen Schadensgefahr" als erfüllt angesehen wird. Das ist bedenklich, weil Geheimnisverrat und Datenmissbrauch in den Unternehmen ständig zunehmen und Schätzungen jährliche Schäden in Deutschland in Milliardenhöhe vermuten.[17] Jeder kleine Ladendiebstahl wird heute unter Bejahung des öffentlichen Interesses angeklagt, bei Datenmissbrauch und Geheimnisverrat in Firmen mit ganz anderen wirtschaftlichen Dimensionen dagegen das öffentliche Interesse oftmals verneint. Das ist nicht nachvollziehbar. Es ist dringend erforderlich, dass die Staatsanwaltschaften eine einheitliche Praxis entwickeln und derartige kriminelle Machenschaften von Firmenmitarbeitern schon aus Gründen der Generalprävention anklagen.[18]

IV. Zivilrechtliche Ansprüche

§ 17 UWG ist nicht nur Strafnorm, sondern auch Schutzgesetz i. S. d. § 823 Abs. 2 BGB. Dadurch werden dem betroffenen Unternehmen Ansprüche gegen den untreuen Mitarbeiter und Dritte, die mitgenommene Daten von diesem erlangt haben, eröffnet.

Gegenüber Wettbewerbern, die die von Mitarbeitern erlangten Betriebsgeheimnisse unbefugt verwerten, gewähren die §§ 3, 4, 8 und 9 UWG darüber hinaus wettbewerbsrechtliche Ansprüche.

Im Einzelnen:

Gegen den untreuen Mitarbeiter und/oder einen Verwerter hat das betroffene Unternehmen Ansprüche aus § 17 UWG i.V.m. § 823 Abs. 1 und 2 BGB, § 1004 BGB auf Unterlassung, Auskunft und Schadensersatz. Gegen beteiligte Wettbewerber stehen dem betroffenen Unternehmen darüber hinaus Ansprüche auf Beseitigung und Unterlassung gemäß § 8 UWG und auf Schadensersatz gemäß § 9 UWG zu. Der Schadensersatz umfasst hierbei

- Auskunft
- Rechnungslegung
- Berichtigung
- Folgenbeseitigung
- Zahlung in Geld.

Die vorgenannten wettbewerbsrechtlichen Ansprüche aus §§ 8 und 9 UWG verjähren gemäß § 11 UWG in der kurzen Frist von sechs Monaten. Die Verjährungsfrist beginnt gemäß dieser Vorschrift, wenn

- der Anspruch entstanden ist und
- der Gläubiger von den anspruchsbegründenden Umständen und der Person des Schuldners Kenntnis erlangt oder ohne grobe Fahrlässigkeit erlangen müsste (§ 11 Abs. 2 UWG).

Die kurze Verjährungsfrist des § 11 UWG gilt jedoch nicht für Schadensersatzansprüche gem. §§ 17 UWG, 823 Abs. 2, 1004 BGB. Für diese gelten die allgemeinen Verjährungsvorschriften des BGB.

In der Praxis bereitet die Geltendmachung der zivilrechtlichen Ansprüche schon deshalb Probleme, weil das geschädigte Unternehmen grundsätzlich die Beweislast trägt.

Gelingt es ihm aufgrund selbst erstellter oder von der Staatsanwaltschaft im Beschlagnahmewege gesicherter Unterlagen, Datenmissbrauch und Geheimnisverrat durch Mitarbeiter zu beweisen, berufen sich Konkurrenzunternehmen in der Regel darauf, sie hätten von der rechtswidrigen Beschaffung dieser Unterlagen durch ihren neuen Mitarbeiter nichts gewusst und seien davon ausgegangen, dass diese ihre Kenntnisse ohne Rechtsbruch erlangt hätten. Gegenüber diesem Einwand hilft dem geschädigten Unternehmen jedoch die Zurechnungslehre des § 831 BGB.

16 Zur sodann eintretenden Beweiserleichterung vgl. nachstehend IV, Ziff. 4

17 Vgl. *Köhler*, in: Köhler/Bornkamm, UWG, 31. Aufl. 2013, Anm. 2 zu § 17

18 Vgl. zum öffentlichen Interesse und Aspekten der Prävention grundsätzlich *Lutz Meyer-Goßner*, StPO, 55. Aufl. 2012, Anm. 7 zu § 153.

Danach wird ein Verschulden des Vorstands/der Geschäftsführung eines Unternehmens in der Form des Organisationsverschuldens bei der Übernahme von führenden oder maßgeblichen Mitarbeitern eines Konkurrenzunternehmens vermutet.[19] Es obliegt dann dem Konkurrenzunternehmen, diese Vermutung zu widerlegen – und zwar mit voller Darlegungslast; ein bloßes Bestreiten reicht nicht aus.

Macht dann ein geschädigtes Unternehmen gegen den Wettbewerber seine zivilrechtlichen Ansprüche geltend, stellen sich Probleme bei der Antragsstellung. Wenn untreue Mitarbeiter geheime Daten mitnehmen und bei ihrer Arbeit beim neuen Arbeitgeber nutzen, kann ihnen bzw. den hiervon profitierenden Unternehmen im Unterlassungsantrag – wie vorstehend unter I. 2. dargelegt – nicht generell der Kontakt mit den jeweiligen Kunden untersagt werden. Vielmehr muss der entsprechende Klageantrag die Untersagung von Wettbewerbshandlungen bei den jeweiligen Kunden unter Verwendung der rechtswidrig erlangten Informationen umfassen. Nimmt man diese Informationen aber in einen entsprechenden prozessualen Unterlassungsantrag auf, erhält das beklagte Unternehmen möglicherweise durch einen solchen Klagantrag gerade diejenigen Informationen, die es bisher nicht oder nur teilweise hatte. Das betroffene Unternehmen liefert dann also im Unterlassungsantrag dem rechtsverletzenden Unternehmen Informationen, die diesem bis dahin nicht zur Verfügung standen. Dennoch kann den Unternehmen in juristischer und betriebswirtschaftlicher Hinsicht nur geraten werden, dieses Risiko in Kauf zu nehmen, weil nur so die weitgehenden zivilrechtlichen Ansprüche auf Unterlassung, Auskunft, Rechnungslegung und Schadensersatz erfolgreich durchgesetzt werden können.

V. Sofortmaßnahmen

In der Praxis hat sich gezeigt, dass veränderungsbereite Mitarbeiter, die zur Konkurrenz wechseln wollen, manchmal bereits während ihrer Tätigkeit Daten des Unternehmens sammeln, die nicht in ihren Tätigkeitsbereich fallen, ihnen nach ihrem Wechsel zum Konkurrenzunternehmen für ihre dortigen Kontakte zu den bisherigen Kunden des betroffenen Unternehmens aber nützlich sind. Meist fällt dies gar nicht auf, weil im Alltagsgeschäft niemand darauf achtet. Es gibt aber Fälle, in denen dies – durch eine wachsame Revision oder auch nur durch Zufall – festgestellt wird, ohne dass die Intention dieses „Sammelns" evident oder auch nur beweisbar ist. Für diesen Vorgang oder die Verwendung unbefugt mitgenommener geheimer Daten durch einen ausgeschiedenen Mitarbeiter sollen nachstehend mögliche Sofortmaßnahmen aufgezeigt werden.

1. Suspendierung/Kündigung

Wenn auch nur erste Belege einer auffälligen, d. h. nicht durch den Aufgabenbereich gedeckten Datensammlung vorliegen, müssen die Verantwortlichen sofort Maßnahmen ergreifen. In der Regel empfiehlt sich zunächst eine vorübergehende Suspendierung des Mitarbeiters unter Sicherung der Beweismittel (Dienst-PC, Datensammlung o.ä.) bis zur Klärung des Vorgangs. Eine solche Maßnahme dürfte arbeitsrechtlich zulässig sein, da die dienstlich nicht veranlasste Datensammlung unter Abwägung der beiderseitigen Interessen als hinreichender Grund für eine Suspendierung anzusehen ist.[20] Für diese Maßnahme ist die Zustimmung eines im Unternehmen etablierten Betriebsrats erforderlich; § 99 Abs. 1 BetrVerfG. Dabei unterliegt ein Betriebsrat hinsichtlich des ihm im Rahmen des Zustimmungsverfahrens vorgelegten Sachverhalts gemäß § 99 Abs. 1, Satz 3 der Schweigepflicht; insoweit empfiehlt sich gemäß § 79 Abs. 1, Satz 1 BetrVerfG ein ausdrücklicher Hinweis.

Wenn es nach vollzogener Suspendierung und ggfs. durchzuführender Anhörung des Mitarbeiter keinen nachvollziehbaren Grund für die unzulässige Datensammlung gibt, ist in der Regel eine ordentliche Kündigung mit sofortiger Freistellung, in gravierenden Fällen eine außerordentliche Kündigung geboten. Eine Abmahnung dürfte regelmäßig entbehrlich sein, da die Vertrauensgrundlage eines Dienstverhältnisses durch unzulässige Datensammlung meist zerstört, jedenfalls aber so sehr beeinträchtigt ist, dass dem Arbeitgeber eine Fortsetzung des Arbeitsverhältnisses bis zu seiner Beendigung nicht zuzumuten ist.[21]

Bei einer außerordentlichen Kündigung ist aber stets die strenge Frist des § 626 Abs. 2 BGB zu beachten. Diese beginnt jedoch erst ab dem Zeitpunkt zu laufen, ab dem der Dienstgeber eine zuverlässige und vollständige Kenntnis vom Kündigungssachverhalt hat.[22]

2. Einstweilige Verfügung

Ist der Arbeitnehmer unter Mitnahme geheimer Daten ausgeschieden und macht er hiervon selbst oder durch Zurverfügungstellung an seinen neuen Arbeitgeber zu Wettbewerbszwecken Gebrauch, ist die sofortige Durchsetzung des nach § 17 UWG eröffneten Unterlassungsanspruchs durch eine einstweilige Verfügung möglich.

In Betracht kommt regelmäßig eine Unterlassungsverfügung gemäß § 940 ZPO, durch die dem Verwender der rechtswidrig mitgenommenen geheimen Daten deren Gebrauch untersagt wird, um wesentliche Nachteile vom betroffenen Unternehmen abzuwenden.

Das Problem dürfte hier regelmäßig in der Glaubhaftmachung des Verfügungsanspruchs liegen, also des Beweises sowohl rechtswidriger Datenentwendung als auch ihres Einsatzes zu Zwecken des Wettbewerbs durch den ausgeschiedenen Mitarbeiter oder den Wettbewerber. Wenn aber der Datenmissbrauch, gegebenenfalls durch Ermittlungen der Staatsanwaltschaft, erwiesen ist, kann der Verwendungsnachweis regelmäßig zunächst nur durch Umsatzvergleiche (vor/nach dem Ausscheiden des Mitarbeiters) und durch Feststellung des zeitgleichen Wechsels von vom ehemaligen Mitarbeiter in seiner neuen Position angesprochenen Kunden zum Wettbewerber versucht werden. Gelingt es auf diese Weise, den Verfügungsanspruch glaubhaft zu machen, werden Verfügungsgrund und Wiederholungsgefahr gemäß § 12 Abs. 2 UWG jedoch vermutet.[23]

In zeitlicher Hinsicht besteht das Erfordernis unverzüglicher gerichtlicher Geltendmachung. Jedes Zögern ist riskant; bereits ein Zuwarten von einem Monat kann die Dringlichkeit entfallen lassen.[24]

VI. Initiative aus Brüssel

Vorstehende Ausführungen behandeln die bestehende Gesetzeslage. De lege ferenda ist aber auch ein von der EU-Kommission vorgelegter Gesetzesvorschlag vom 28.11.2013 von Bedeutung, demzufolge europäische Unternehmen sich künftig besser vor Diebstahl von Geschäftsgeheimnissen und vertraulichem Know-how schützen können. Zentrale Anliegen sind eine einheitliche Klärung des Begriffs „Betriebsgeheimnis" und sogar die Möglichkeit, Geschäftsgeheimnisse offenbarende Produkte

19 Vgl. *Palandt*, BGB, 73. Aufl. 2014, Anm. 10 zu § 831; BGH, 12.7.1996 – V ZR 280/94, NJW 1996, 3205, 3207.
20 Vgl. hierzu KR-*Lipke*, 10. Aufl. 2013, Anm. 42 zu § 620 BGB.
21 Vgl. hierzu KR-*Fischermeier*, 10. Aufl. 2013, Anm. 169 zu § 626 BGB.
22 Vgl. KR-*Fischermeier*, 10. Aufl. 2013, Anm. 319 zu § 626 BGB.
23 Vgl. *Baumbach/Lauterbach*, ZPO, 70. Aufl. 2012, Anm. 10 zu § 940.
24 Vgl. *Baumbach/Lauterbach*, ZPO, 70 Aufl. 2012, Anm. 6 zu § 940.

vom Markt zu nehmen. Der Kommissionsvorschlag soll demnächst dem Ministerrat und dem Europäischen Parlament zur Verabschiedung im ordentlichen Gesetzgebungsverfahren übermittelt werden.[25]

VII. Fazit

1. Geheimnisverrat und Datendiebstahl durch Mitarbeiter kommen in der Praxis häufiger vor, als Unternehmer annehmen. Oft werden sie gar nicht oder zu spät bemerkt; ebenso oft zögern die Unternehmen, juristische Maßnahmen zu ergreifen. Dabei hilft § 17 UWG; aber wie bei jeder Vorschrift, die in Rechte anderer eingreift, bestehen strenge Darlegungsvoraussetzungen und Beweisanforderungen. In Anbetracht erheblicher Schäden, die die deutsche Wirtschaft jährlich durch Datenmissbrauch und Geheimnisverrat erleidet,[26] kann man jedem Unternehmer nur raten, hinsichtlich solcher Mitarbeiter-Delikte wachsam zu sein und, wenn sie festgestellt werden, sofort die gebotenen juristischen Maßnahmen zu ergreifen.
2. Im Interesse der Wirtschaft ist eine baldige Umsetzung der EU-Gesetzesinitiative zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in geltendes Recht wünschenswert.

Dr. jur. Michael Fingerhut ist seit 1972 Rechtsanwalt und seit 1995 Seniorpartner der Kanzlei FINGERHUT RECHTSANWÄLTE in München. Der Schwerpunkt seiner Tätigkeit liegt im Bereich des Wirtschaftsrechts und der Beratung mittelständischer Unternehmen. Nebenberuflich arbeitet Dr. Fingerhut seit 1992 als Referent für Rechtsseminare bei der IHK-Akademie für München und Oberbayern und bei Inhouse-Seminaren in Unternehmen.

25 Vgl. hierzu ausführlich BB 2013, 3010, Stichwort Verwaltung; ferner die Presse-Mitteilung der EUKommission vom 28.11.2013.
26 Die Schätzungen gehen in die Milliarden; vgl. *Köhler*, in: Köhler/Bornkamm, UWG, 31. Aufl. 2013, Anm. 2 zu § 17.