LAUTERKEITS- UND IMMATERIALGÜTERRECHT

OGH: Verletzung von Geschäftsgeheimnissen durch Ausnützen von Sicherheitslücken

1. **Der für die Anwendung von § 11 UWG maßgebende Geheimhaltungswille muss nicht ausdrücklich erklärt werden, sondern kann sich auch aus den Umständen ergeben.**
2. **Der Geheimhaltungswille ist ausreichend erkennbar, wenn sich aus dem Verhalten des Unternehmers ergibt, dass bestimmte – auch sonst nicht allgemein zugängliche – Informationen einem bestimmten Personenkreis vorbehalten sein sollen. Das ist bei einer durch ein Passwort geschützten Datenbank der Fall.**
3. **Mangelhafte Sicherheitsstandards („Sicherheitslücken") erlauben bei aufrechtem Passwortschutz nicht den Schluss, dass der Unternehmer kein Interesse an der Geheimhaltung hätte.**
4. **Faktische Verfügungsmacht und eigenes Geheimhaltungsinteresse genügen für die Annahme, dass an sich fremde Daten (auch) eigene Geschäftsgeheimnisse sind, die in den Schutzbereich des § 11 Abs 2 UWG fallen.**

Redaktionelle Leitsätze

OGH Beschluss vom 25.10.2016,
4 Ob 165/16t – *Ticketsysteme*

Deskriptoren: Geschäftsgeheimnis, Geheimhaltungswille, Umgehung von Passwortschutz, Sicherheitslücken.

Normen: §§ 11, 13 UWG.

Aus den Entscheidungsgründen

Die Parteien erzeugen und vertreiben Ticket- und Eintrittssysteme für Skigebiete, Stadien und ähnliche Einrichtungen. Die Klägerin betreibt zudem Server, auf denen interne Anwendungen für ihre Kunden installiert sind. Sie speichert dort die mit der Nutzung der Eintrittssysteme verbundenen Daten ihrer Kunden, die online Zugang zu den Daten über eine passwortgeschützte Datenbank haben. Insbesondere können sie die Daten in Form von Berichten (etwa über Name und Anschrift der Käufer von Tickets in einem bestimmten Zeitraum) abrufen.

Solche Berichte wurden am Server, auf dem die Anwendung für den Kunden installiert war, standardmäßig in einem Zwischenspeicher („Cache") abgelegt. Bei einigen dieser Server war es aufgrund der Verwendung einer Standardeinstellung möglich, unter Umgehung des Log-in-Vorgangs (mit Benutzername und Passwort) auf den Zwischenspeicher zuzugreifen. Dieser Zugriff erforderte jedoch mehrere Informationen, die einem Außenstehenden nicht bekannt waren und nur von IT-Spezialisten durch gezieltes Auskundschaften und Zuhilfenahme von Spezialsoftware erlangt werden konnten.

Für einen unautorisierten Zugriff auf die Berichte waren nicht öffentliche Informationen erforderlich, die durch gezieltes Erkunden und Abfragen und eine gezielte Suche nach Schwachstellen im Sicherheitssystem der betroffenen Server gewonnen werden konnten. Diese Informationen waren vertraulich und von der Klägerin nicht veröffentlicht worden.

Anfang 2015 begann ein Mitarbeiter der Beklagten, unter Umgehen des Kennwortschutzes auf die betroffenen Server zuzugreifen. Die Benutzernamen und Kennwörter waren ihm von den Kunden der Klägerin nicht zur Verfügung gestellt worden. Bei einer „Mitbewerberanalyse" hatte er bei einem dieser Kunden eine Bildschirmanzeige fotografiert, der eine bestimmte Internetadresse (URL) entnommen werden konnte. Nach dem Vorbringen der Beklagten konnten aufgrund dieser URL mit „trial and error" unter geringfügiger Modifikation der IP-Adresse und Verwendung bestimmter Programmbefehle auch Berichte anderer Kunden abgefragt werden. Ob der Mitarbeiter die Bildschirmanzeige mit Zustimmung des Kunden fotografiert hatte, konnten die Vorinstanzen nicht feststellen.

Insgesamt griff der Mitarbeiter der Beklagten zumindest zwölfmal auf Daten verschiedener Kunden der Klägerin

zu, wobei er jeweils Befehle eingab, die zur Erstellung von Berichten führten.

Die Beklagte verwertete die durch die Zugriffe erhaltenen Informationen gezielt dazu, Kunden der Klägerin abzuwerben und der Klägerin beim Anwerben von Neukunden fehlende Datensicherheit, also dass Daten „frei im Internet" zugänglich wären, zu unterstellen.

Zur Sicherung ihres gleichlautenden Unterlassungsbegehrens beantragt die Klägerin, der Beklagten mit einstweiliger Verfügung zu verbieten, die widerrechtlich aus der Verfügungsmacht der Klägerin erlangten Daten zu nutzen und/oder nutzen zu lassen und oder gegenüber Dritten zu offenbaren.

Das Erstgericht erließ die einstweilige Verfügung. Die Beklagte habe „sittenwidrig" iSv § 1 UWG gehandelt, weil sie widerrechtlich erlangte Daten benutzt habe, um die Klägerin anzuschwärzen. Darin liege auch eine Verletzung von Betriebs- und Geschäftsgeheimnissen iSv § 11 Abs 2 UWG. Die rechtswidrigen Zugriffe auf die Server und die Verwendung und Weitergabe von Daten fielen zudem in die Fallgruppe „Wettbewerbsvorsprung durch Rechtsbruch" und verstießen daher auch gegen § 1 UWG.

Das Rekursgericht bestätigte diese Entscheidung. Bei den mit Benutzername und Passwort geschützten Daten habe es sich um Geheimnisse iSv § 11 Abs 2 UWG gehandelt. Da die Zustimmung des Kunden zum Abfotografieren der Bildschirmanzeige nicht bescheinigt sei, sei jedenfalls von einem unlauteren Erlangen der Informationen auszugehen. Die Daten hätten sich in der faktischen Verfügungsmacht der Klägerin befunden. Die Beklagte habe die Daten unbefugt zu Zwecken des Wettbewerbs verwertet.

Der gegen diese Entscheidung gerichtete außerordentliche Revisionsrekurs der Klägerin ist zulässig, weil die Rechtslage einer Klarstellung bedarf, er ist aber nicht berechtigt.

1. Nach § 11 Abs 2 UWG iVm § 13 UWG kann auf Unterlassung in Anspruch genommen werden, wer „Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er [...] durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbs unbefugt verwertet oder an andere mitteilt."

2. Bei den strittigen Daten handelte es sich um Geschäftsgeheimnisse.

2.1. Betriebs- oder Geschäftsgeheimnisse sind Tatsachen und Erkenntnisse kommerzieller oder technischer Art, die bloß einer bestimmten und begrenzten Zahl von Personen bekannt sind, nicht über diesen Kreis hinausdringen sollen und an deren Geheimhaltung ein wirtschaftliches Interesse besteht (9 Os 7/70, SSt 41/32; RIS-Justiz RS0079599; zuletzt etwa 4 Ob 55/14p, *Betriebsgeheimnisse*). Der Geheimhaltungswille muss nicht ausdrücklich erklärt werden, sondern kann sich auch aus den Umständen ergeben; im Anwendungsbereich des § 11 Abs 1 UWG (Geheimnisverletzung durch Bedienstete) genügt es, dass sich ein durchschnittlicher Arbeitnehmer über diesen Willen des Unternehmers klar sein musste (4 Ob 394/86, *Tenniskartei*, ÖBl 1988, 13; RIS-Justiz RS0079599 [T1]; zuletzt etwa 4 Ob 55/14p, *Betriebsgeheimnisse*). Gleiches muss bei der Verletzung von Geschäftsgeheimnissen durch Dritte (§ 11 Abs 2 UWG) gelten. Auch hier genügt es daher, wenn sich aus dem Verhalten des Unternehmers ergibt, dass bestimmte – auch sonst nicht allgemein zugängliche – Informationen einem bestimmten Personenkreis vorbehalten sein sollen.

2.2. Diese Voraussetzung ist bei Daten erfüllt, die regulär nur durch das Einloggen in eine durch Passwort geschützte Datenbank eingesehen werden können. Denn diese Schutzvorkehrungen lassen erkennen, dass die Kenntnis dieser Daten einem bestimmten Personenkreis vorbehalten sein sollte. Der für die Anwendung von § 11 UWG maßgebende Geheimhaltungswille ist daher ohne weiteres erkennbar. Aus „Sicherheitslücken", wie sie hier offenbar vorlagen, lässt sich nichts Gegenteiliges ableiten. Denn mangelhafte Sicherheitsstandards erlauben bei aufrechtem Passwortschutz nicht den Schluss, dass der Unternehmer kein Interesse an der Geheimhaltung mehr hätte. Vielmehr müssen sowohl Beschäftigte (§ 11 Abs 1 UWG) als auch Dritte (§ 11 Abs 2 UWG) redlicherweise annehmen, dass dem Unternehmer diese Mängel nicht bewusst waren, sodass aus deren Vorliegen keinesfalls ein Wegfall des Geheimnischarakters abgeleitet werden kann.

2.3. Die am 5. Juli 2016 in Kraft getretene und bis 9. Juni 2018 umzusetzende RL (EU) 2016/943 *über den Schutz vertraulichen Knowhows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung* steht dieser Auffassung nicht entgegen. Die Beklagte stützt sich insofern auf Art 2 Abs 1 lit c dieser RL, wonach Informationen ua nur dann als „Geschäftsgeheimnis" im Sinn der RL gelten, wenn sie „Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person [sind], die die rechtmäßige Kontrolle über die Informationen besitzt."

Diese Argumentation scheitert aus zwei Gründen.

(a) Zum einen ist die Umsetzungsfrist noch nicht abgelaufen. Zwar darf das nationale Recht auch vor diesem Zeitpunkt (soweit möglich) nicht in einer Weise ausgelegt werden, die das Erreichen des mit der Richtlinie verfolgten Zieles ernsthaft gefährden würde (C-212/04, *Adeneler*, Rz 123). Damit wird allerdings auch nach

Auffassung des EuGH kein Gebot richtlinienkonformer Auslegung schon vor Ablauf der Umsetzungsfrist begründet (C-212/04, *Adeneler*, Rz 115; ebenso *Nettesheim* in *Grabitz/Hilf/Nettesheim*, Das Recht der Europäischen Union, Art 288 Rz 133; *Vcelouch* in *Mayer/Stöger*, EUV/AEUV, Art 288 AEUV Rz 62). Dass die bisherige Interpretation des Begriffs „Geschäftsgeheimnis" das Erreichen der mit der Richtlinie verfolgten Ziele ernsthaft gefährdete, ist nicht erkennbar.

(b) Zum anderen können die Mitgliedstaaten auch nach Ende der Umsetzungsfrist nach Art 1 Abs 1 der RL einen weitergehenden Schutz von Geschäftsgeheimnissen vorsehen. Zwar gilt das nicht, wenn das weitergehende nationale Recht gegen bestimmte Vorschriften der Richtlinie verstieße. Es ist aber nicht erkennbar, dass dies bei der hier maßgebenden Interpretation des Begriffs „Geschäftsgeheimnis" zuträfe. Insbesondere ist die zwingende Schutzausnahme nach Art 5 lit b der RL im konkreten Fall nicht anwendbar. Danach ist zwar das Offenlegen von Geschäftsgeheimnissen zur Aufdeckung eines „beruflichen Fehlverhaltens" zulässig; dies allerdings nur dann, wenn es in der Absicht erfolgt, „das allgemeine öffentliche Interesse zu schützen". Im Gegensatz dazu hat die Beklagte hier ausschließlich eigene Interessen verfolgt.

(c) Aus diesen Gründen ist nicht weiter zu prüfen, ob unbeabsichtigte Sicherheitslücken tatsächlich nach Art 2 Abs 1 lit c der RL das Vorliegen eines Geschäftsgeheimnisses *im Sinn dieser RL* ausschließen.

3. Bei den strittigen Daten handelt es sich (auch) um Geschäftsgeheimnisse der Klägerin.

Zwar stammen die Daten von ihren Kunden und beziehen sich auf deren geschäftliche Verhältnisse. Faktisch befanden sie sich jedoch in der Verfügungsmacht der Klägerin, und sie hatte auch ein erhebliches eigenes Interesse an deren Geheimhaltung, da sonst die Nichtverlängerung der Verträge oder Schadenersatzansprüche der Kunden (*Juranek/Stögerer*, Sicherheitslücken in der Unternehmens-EDV und Haftungskonsequenzen, ecolex 2015, 955) drohten. Faktische Verfügungsmacht und eigenes Geheimhaltungsinteresse genügen bei wertender Betrachtung für die Annahme, dass die Daten auch in Bezug auf die Klägerin in den Schutzbereich des § 11 Abs 2 UWG fallen.

4. An der Rechtswidrigkeit des Erlangens der Daten (§ 11 Abs 2 UWG) durch Eindringen in das fremde Computersystem besteht kein Zweifel (6 Ob 126/12s, jusIT 2013/26 [*Staudegger*] = ZIR 2013, 224 [*Dörfler*]). Die Beklagte hat nach Erkennen der Sicherheitslücke gezielt auf verschiedene Server der Klägerin und eines von dieser betreuten Unternehmens zugegriffen und von dort Daten, die faktisch in der Verfügungsmacht der Klägerin als EDV-Dienstleisterin waren, in verarbeiteter Form heruntergeladen. Die Beklagte stützt sich für die ihrer Ansicht nach dennoch fehlende Rechtswidrigkeit ausschließlich auf die Negativfeststellung zur Frage, ob ein Kunde einem Mitarbeiter der Beklagten das Abfotografieren der Bildschirmanzeige erlaubt habe oder nicht. Darauf kommt es aber nicht an. Denn selbst wenn der Kunde diese Erlaubnis erteilt hätte, folgte daraus nicht seine Zustimmung zu einer dadurch möglich werdenden Abfrage seiner Daten. Zudem hatte der Mitarbeiter der Beklagten die durch das Abfotografieren erhaltenen Informationen auch zum Zugriff auf Daten von anderen Kunden der Klägerin genutzt. Dies konnte keinesfalls von der allfälligen Zustimmung durch den einen Kunden gedeckt sein.

5. Das Verwerten und Weitergeben der Daten bestreitet die Beklagte nicht. Damit besteht der Unterlassungsanspruch der Klägerin schon nach § 11 Abs 2 iVm § 13 UWG zurecht. Der Revisionsrekurs der Beklagten muss daher scheitern, ohne dass zu prüfen wäre, ob der Anspruch auch nach § 1 UWG begründet wäre (Wettbewerbsvorsprung durch Rechtsbruch wegen Verstoß gegen Datenschutz- oder Strafrecht; Verletzung der beruflichen Sorgfalt).

Anmerkung

Von Maximilian Kralik

Dass die Umgehung von – wenngleich offenbar unzureichenden – Sicherheitsmaßnahmen zur Beschaffung fremder Daten und die anschließende Verwertung dieser Daten zur Abwerbung von Kunden des Mitbewerbers, unlauter ist, ist einleuchtend.

Nicht neu ist, dass sich der Geheimhaltungswille auch aus den Umständen ergeben kann (OGH 19.05.1987, 4 Ob 394/86). Demzufolge ist es konsequent, dass auch Daten einer passwortgesicherten Datenbank, die in einer für einen durchschnittlichen Beschäftigten erkennbaren Weise nicht über den Kreis der Berechtigten hinaus (der Allgemeinheit) bekannt werden und daher der Geheimhaltung unterliegen sollen, Geschäftsgeheimnisse darstellen. Ob Sicherheitslücken einen Zugriff durch Unberechtigte zulassen, kann nach aktueller

Rechtslage für die Frage des Vorliegens des Geheimhaltungswillens nicht entscheidend sein. Es ist daher auch nicht relevant, ob ein Mitarbeiter der beklagten Partei die Bildschirmanzeige, die die Sicherheitslücke offenbart hat, mit Zustimmung eines Kunden abfotografiert hat oder nicht. Anders wäre der Fall wohl zu beurteilen, wenn die Klägerin im Wissen um die unzureichenden Sicherheitsmaßnahmen diesen Zustand nicht geändert hätte – dann wäre der Schluss wohl zulässig, dass die Klägerin kein Interesse an der Geheimhaltung mehr hätte.

Der OGH lässt allerdings die Frage offen, ob unbeabsichtigte Sicherheitslücken nach Art 2 Abs 1 lit c der Know-how-Richtlinie (Richtlinie „über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen [Geschäftsgeheimnisse] vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung", [EU] 2016/943) das Vorliegen eines Geschäftsgeheimnisses im Sinn der RL ausschließen. Gemäß Art 2 Abs 1 lit c der RL sind Geschäftsgeheimisse Informationen, die ua „Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt", sind; was „angemessene" Geheimhaltungsmaßnahmen sind, lässt die RL offen. Diese Voraussetzung ist jedenfalls in Österreich neu und sie erfordert in Zukunft (die Umsetzungsfrist endet erst 2018, konkrete Umsetzungsvorschläge liegen noch nicht vor), dass Unternehmer Geschäftsgeheimnisse aktiv schützen – ein Rückgriff auf die Umstände, die den Geheimhaltungswillen erkennen lassen, ist dann möglicherweise nicht mehr möglich.

Als Geheimhaltungsmaßnahmen, wie sie der Richtlinientext fordert, können gleichermaßen eigene technische und organisatorische Maßnahmen (Zutritts-, Zugangs- und Zugriffskontrollen), wie auch Maßnahmen vertraglicher Art (Geheimhaltungsvereinbarungen, non-disclosure agreements bzw confidential disclosure agreements und insb Geheimhaltungsklauseln in Arbeits- und Werkverträgen) verstanden werden. Sämtliche Maßnahmen müssen gut dokumentiert sein, damit sie in einem etwaigen Verletzungsprozess auch beweisbar sind.

Der Hinweis des OGH, wonach sich der Geheimhaltungswille auch aus den Umständen ergeben kann, deutet zwar auf einen weiten Schutzbereich für Geschäftsgeheimnisse hin. Das in der Know-how-Richtlinie enthaltene Erfordernis der angemessenen Geheimhaltungsmaßnahmen sollte in der Praxis jedoch bereits jetzt beachtet werden und es sollten entsprechende IT-Maßnahmen gesetzt sowie interne Richtlinien und Verträge entsprechend gestaltet oder geändert werden.

Dass jedwede Sicherheitslücke das Vorliegen eines Geschäftsgeheimnisses ausschließt, kann jedenfalls nicht die Folge der Richtlinie sein. Letztlich wird es in einem Verfahren auf die Abwägung zwischen den gesetzten und nachgewiesenen (!) Geheimhaltungsmaßnahmen des Unternehmers und der Schwere der Sicherheitslücke bzw den Anforderungen an die Umgehung von Schutzmaßnahmen ankommen.

Die Frage, wessen Geschäftsgeheimnisse streitgegenständlich verletzt wurden, beantwortet der OGH richtig: Es handelt sich (auch) um Geschäftsgeheimnisse der Klägerin, denn die Daten befanden sich (auch) in ihrer Verfügungsmacht und sie hatte (auch) ein eigenes Geheimhaltungsinteresse. Das eigene Geheimhaltungsinteresse begründet der OGH damit, dass ohne Geheimhaltung die Nichtverlängerung der Verträge oder Schadenersatzansprüche drohten. Darüber hinaus enthalten Daten in der Regel wertvolle Informationen über die eigenen Produkte und Dienstleistungen, die – richtig interpretiert und genützt – zur Verbesserung der eigenen Leistungen am Markt genützt werden können. Mit den Worten der Richtlinie ausgedrückt, handelt es sich daher um Informationen, „bei denen sowohl ein legitimes Interesse an ihrer Geheimhaltung besteht als auch die legitime Erwartung, dass diese Vertraulichkeit gewahrt wird" (Erwägungsgrund 14).

Und noch ein letzter Gedanke zu den Schutzausnahmen der Know-how-Richtlinie: Gemäß Art 5 lit b liegt keine Verletzung von Geschäftsgeheimnissen vor, wenn der Erwerb oder die Nutzung der Geschäftsgeheimnisse „zur Aufdeckung eines beruflichen oder sonstigen Fehlverhaltens oder einer illegalen Tätigkeit [erfolgt ist], sofern der Antragsgegner in der Absicht gehandelt hat, das allgemeine öffentliche Interesse zu schützen."

Auch hier stellt sich die Frage, ob eine Sicherheitslücke, die jedoch nur für eine Fachper-

son erkennbar ist, bereits ein berufliches Fehlverhalten iSd Know-how-Richtlinie begründet. Im Hinblick auf Erwägungsgrund 20 der Richtlinie geht es bei dieser Schutzausnahme darum, Whistleblowing-Aktivitäten zu schützen. Unternehmer sollen sich bei eigenem Fehlverhalten nicht auf den Schutz von Geschäftsgeheimnissen stützen können; umgekehrt sollen Whistleblower vor rechtlichen Konsequenzen geschützt sein. Damit ist auch – wie der OGH richtig erkannt hat – der Anwendungsbereich der Schutzausnahme, der eng auszulegen sein wird, abgesteckt: Zum einen fällt wohl nur ein solches Fehlverhalten in den Anwendungsbereich der Ausnahme, das öffentliche Interessen beeinträchtigt (also eklatante Verstöße oder strukturelle Missverhältnisse); geringfügige Sicherheitslücken in Datenbanken fallen wohl nicht darunter. Zum anderen ist das Aufdecken von Geschäftsgeheimnissen nur zum Schutz allgemeiner öffentlicher Interessen zulässig; die Abwerbung von Kunden des Mitbewerbers fällt ganz offensichtlich nicht darunter. Völlig zutreffend ist daher auch die Schutzausnahme der Richtlinie nicht anwendbar; völlig unabhängig davon, dass die Umsetzungsfrist für die Richtlinie noch nicht abgelaufen ist.