

Kein Fernmeldegeheimnis am Arbeitsplatz?

Spannungsfeld zwischen Datenschutz und Compliance-Maßnahmen

Dr. Christiane Bierekoven, Associate Partner und Leiterin des IT Kompetenzcenter, Rödl & Partner

Ein aktuelles Urteil nimmt sich der Frage an, ob private E-Mails auf dem Firmen-PC generell unter den Schutz des Telekommunikationsgesetzes fallen oder nicht. Die Einzelfallentscheidung enthält überraschenden Zündstoff.

Anlass des Urteils war eine Aufforderung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) an die Klägerin. Die BaFin wollte im Wege der Amtshilfe für die US-amerikanische Wertpapieraufsichtsbehörde SEC wegen des Verdachts von Insidergeschäften auf der Grundlage von § 4 Abs. 3 WpHG mit Bescheid vom 18.4.2007 u.a. die Klägerin dazu bringen, sämtliche E-Mails namentlich bezeichneter Mitarbeiter, die bestimmte Namen und Stichworte oder E-Mail-Adressen enthielten, vorzulegen. Die Klägerin, die ihren Mitarbeitern die private E-Mail- und Internetnutzung erlaubt hatte, weigerte sich unter Berufung auf das Fernmeldegeheimnis des § 88 TKG, Art. 10 Abs. 1 GG. Das VG Frankfurt a.M. verneinte in Urt. v. 6.11.2008 – 1 K 628/08 einen dahingehenden Eingriff.

Fernmeldegeheimnis vs. strafrechtliche Aufklärung

Eine Verletzung des Fernmeldegeheimnisses liegt nach Auffassung des VG Frankfurt a.M. nicht vor, wenn Mitarbeiter wie vorliegend die Möglichkeit haben, selbst zu entscheiden, ob sie E-Mails, die auf dem Firmenserver nach sechs Wochen gelöscht werden, auf der Festplatte ihres Arbeitsplatzrechners zu speichern. Zur Begründung führt

das Gericht im Wesentlichen an, nach der Entscheidung des BVerfG vom 2.3.2006, Az 2 BvR 2099/04 schütze das Fernmeldegeheimnis die Vertraulichkeit der privaten Korrespondenz ausschließlich auf dem Übertragungsweg gegen unbefugten und unbeherrschbaren Zugriff Dritter.

Dieser Schutz ende, sobald die Nachricht beim Empfänger angekommen und der Übertragungsvorgang beendet sei. In diesem Moment könne der Empfänger eigene Schutzvorkehrungen treffen. Die Nachricht sei nicht mehr den erleichterten Zugriffsmöglichkeiten Dritter ausgesetzt. Vielmehr unterschieden sich die anschließend gespeicherten Inhalte und Verbindungsdaten nicht mehr von Dateien, die der Nutzer selbst angelegt habe. Dies gelte auch, wenn und soweit solche E-Mails auf dienstlichen Rechnern gespeichert würden. Hierdurch befänden sie sich zwar weiterhin im Herrschaftsbereich des Arbeitgebers, jedoch seien die Berechtigten nicht mehr den spezifischen Zugriffsgefahren des Übertragungsweges ausgesetzt. Vielmehr habe der Berechtigte es selbst in der Hand, diese E-Mails zu löschen. Entscheide er sich für eine Speicherung an einer selbst gewählten Stelle im Telekommunikationssystem des Arbeitgebers, stehe ihm dafür ein unbefristeter Schutz durch das

Fernmeldegeheimnis nicht mehr zur Seite.

Bedeutung für die Unternehmenspraxis

Das Gericht setzt sich als erstes mit der äußerst schwierigen und strittigen Problematik der Reichweite des Fernmeldegeheimnisses des § 88 TKG, Art. 10 Abs. 1 GG bei zugelassener privater E-Mail- und Internetnutzung am Arbeitsplatz im Spannungsfeld zu internen strafrechtlichen Aufklärungs- und Präventionsmaßnahmen auseinander. Sie ist dennoch unbefriedigend, da sie die typischen in der Praxis auftretenden Probleme nicht beantwortet. Bislang besteht in der juristischen Fachliteratur weitgehend Einigkeit, dass ein Arbeitgeber, der seinen Mitarbeitern die private E-Mail- und Internetnutzung erlaubt, als Telekommunikationsdiensteanbieter nach § 88 Abs. 2 i.V.m. § 3 Nr. 6, 10 TKG anzusehen und deswegen an das Fernmeldegeheimnis des § 88 TKG gebunden ist. Unstreitig ist weiterhin, dass deswegen ohne Einwilligung der Mitarbeiter eine inhaltliche Kontrolle der privaten E-Mail Korrespondenz unzulässig ist. Was aber gilt, wenn der Arbeitgeber den Verdacht hat, dass seine Mitarbeiter strafrechtlich relevante Handlungen, insbeson-

dere per E-Mail, begehen, ist ungeklärt. Vielfach wird empfohlen, in diesen Fällen den internen Datenschutzbeauftragten, ggf. ein Mitglied des Betriebsrates, hinzuziehen und die E-Mails gemeinsam mit dem betroffenen Mitarbeiter anzuschauen oder zuvor gemeinsam mit dem Mitarbeiter private und dienstliche E-Mails zu trennen (für letztere Variante beispielsweise Göpfert, Merten, Siegrist, NJW 2008, 1703).

Beide Vorgehensweisen bergen aus der Sicht des Unternehmers, der Straftaten aufklären oder verhindern will, jedoch das Risiko, dass der Mitarbeiter, der im Verdacht steht, strafrechtlich relevante Handlungen begangen zu haben, vor einer gemeinsamen Separierung oder vor einem gemeinsamen Anschauen sämtliche strafrechtlich relevanten E-Mails löscht und so jegliche Beweismittel vernichtet. Eine Aufklärung ist dem Unternehmer auf diese Weise ebenso wenig möglich wie eine effektive und effiziente Prävention. Diese Vorgehensweise wird deshalb in der Praxis häufig als untauglich erachtet und kritisiert. Andererseits müssen Unternehmen unter Compliance-Gesichtspunkten die Möglichkeit haben, E-Mails ihrer Mitarbeiter bei Vorliegen von Verdachtsmomenten auf Straftaten inhaltlich zu prüfen, um diese aufzudecken, zu sanktionieren und weitere zu verhindern, um sich nicht als Unternehmen „strafbar“ zu machen. Ungeklärt ist bislang auch, ob eine inhaltliche Prüfung nur dann zulässig ist, wenn Straftaten per E-Mail begangen wurden oder auch dann, wenn die E-Mails „lediglich“ als Beweismittel für strafbare Handlungen in Betracht kommen. Ebenso ungeklärt ist, wie konkret die Anhaltspunkte für den Verdacht einer Straftat sein müssen, um einen Eingriff in das Fernmeldegeheimnis zu rechtfertigen. Denkbar wäre angelehnt an die strafrechtliche Terminologie eine Art Anfangs- oder dringender Tatverdacht.

All diesen Fragen geht das VG Frankfurt a. M. nicht nach und beantwortet sie auch nicht in seiner vorgenannten Entscheidung. Diese macht es sich einfach, indem es bereits die Verletzung des Fernmeldegeheimnisses verneint. Sollten sich andere Gerichte seiner Auffassung anschließen, würde in all den Fällen der Schutz des Fernmeldegeheimnisses nicht greifen, in denen Unternehmen Arbeitnehmern die Möglichkeit geben, ihre privaten E-Mails auf dienstlichen Rechnern zu speichern. Dies erscheint schon deswegen bedenklich, weil das Gericht das sodann greifende Recht auf informationelle Selbstbestimmung außer Acht lässt. Zudem bleibt offen, ob und welchen Schutz die privaten E-Mails gehabt hätten, wenn sie zum Zeitpunkt der Vorlageanforderung noch auf dem Server des Arbeitgebers gespeichert gewesen wären, was zwar vorliegend nicht der Fall war, aber eine weit verbreitete Praxis in Unternehmen darstellt.

Fazit

Angesichts dessen, dass das VG Frankfurt a. M. die meisten der in der Praxis im Zusammenhang mit dem Zugriff auf private E-Mails des Arbeitnehmers relevanten Fragen außer Acht lässt, sollte diese Entscheidung derzeit nicht überbewertet werden. Sie ist zudem bislang eine Einzelfallentscheidung geblieben, die wesentliche Aspekte unberücksichtigt lässt. Die Einführung eines Arbeitnehmerdatenschutzrechtes wurde jüngst – jedenfalls für die aktuelle Legislaturperiode – von der Bundesregierung abgelehnt. Die Rechtslage bleibt also weiterhin unklar. Deshalb empfiehlt es sich in der Praxis, entweder die private Nutzung von E-Mail und Internet gänzlich zu untersagen oder eindeutig und detailliert zu regeln. Hierbei sollte besonderer Wert auf die Formulierung der Einwilligungserklärungen gelegt werden. Diese sollten möglichst genau beschrei-

ben, bei welchen oder welcher Art von Straftaten und bei welchem Grad an Verdachtsmomenten ohne Vorankündigung eine inhaltliche Kontrolle durch den Arbeitgeber erfolgen darf. Sollte der Arbeitnehmer dem nicht zustimmen, kann ihm die private Nutzung insgesamt untersagt werden. Ebenso sollte der betriebliche Datenschutzbeauftragte beteiligt werden. Zu beachten ist zudem, dass solche Maßnahmen nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig sind. Diese Mitbestimmungspflicht gilt für die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten der Arbeitnehmer zu überwachen. In der geschilderten Konstellation dient die IT-Infrastruktur, namentlich die Bereitstellung der E-Mail-Infrastruktur, der Überwachung der Arbeitnehmer.