Exposé

Vorläufiger Titel der Dissertation

„Rechtsprobleme im Umgang mit privaten Daten ausgeschiedener Arbeitnehmer“

Verfasserin

Mag. Alexandra Schrott, LL.M.

angestrebter akademischer Grad

Doktorin der Rechtswissenschaften (Dr. iuris)

Wien, Juni 2015

Studienkennzahl lt. Studienblatt:	A 783 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuer:	Univ.-Prof. Dr. Dietmar Jahnel

Inhaltsverzeichnis

1. Darstellung des Dissertationsvorhabens 3

2. Forschungsstand und Methodik 5

3. Vorläufiges Inhaltsverzeichnis 6

4. Zeitplan 7

5. Vorläufiges Literaturverzeichnis 8

1. Darstellung des Dissertationsvorhabens

Oft wird das Problem erst bewusst, wenn der Arbeitnehmer[1] schon aus dem Unternehmen ausgeschieden ist und nicht mehr gefragt werden kann: In seinem E-Mail-Account befindet sich eine E-Mail eines Kunden und auf seinem privaten Speicherplatz auf dem Server (H:-Ordner) ist noch eine Word-Datei gespeichert, die für den Abschluss eines Auftrages nun dringend erforderlich sind. Sind hier aber vielleicht nicht auch private Daten des Arbeitnehmers gespeichert, auf die der Arbeitgeber unter Umständen gar nicht zugreifen darf? Viele Unternehmen lassen bereits die private Nutzung von dienstlichen E-Mailadressen und Internet zu. Obwohl es meist entsprechende Einzel- oder Betriebsvereinbarungen gibt, bestehen in der Praxis derzeit noch nicht ausjudizierte Rechtsprobleme, insbesondere bei den Fragen, was nach dem Ausscheiden eines Arbeitnehmers mit dessen privaten Daten zu geschehen und wer darauf Rechte hat. Nachfolgend einige Fälle und Fragestellungen, die im Rahmen dieser Dissertation beantwortet werden:

- Der ausgeschiedene Arbeitnehmer war Kundenbetreuer; sein Arbeitgeber will weiterhin den Mailaccount offen lassen, der Arbeitnehmer wehrt sich jedoch dagegen.
- Forderung des ausgeschiedenen Arbeitnehmers an den Arbeitgeber die privaten E-Mails, die zulässig waren, physisch zu löschen, wozu der Arbeitgeber jedoch faktisch nicht in der Lage ist.
- Darf auf „*privat*“ bezeichnete Unterordner des Arbeitnehmers im E-Mailsystem im Rahmen von Untersuchungen zur Aufklärung eines verwaltungs- oder strafrechtlichen Verstoßes zugegriffen werden?
- Dürfen wichtige dienstliche Daten nach dem Tod des Arbeitnehmers auf einem als „*persönlichen Speicherplatz*“ bezeichneten Speicherort gesucht werden?
- Bei Tod eines Arbeitnehmers ist fraglich, wer die Herausgabe der Daten aus dem privaten Speicherplatz sowie aller privater E-Mails vom Mailserver des Arbeitgebers fordern kann („*digitaler Nachlass*“).
- Ein gekündigter Arbeitnehmer behindert die Durchführung forensischer Untersuchungen bei Korruptionsverdacht mit dem Argument, dass sich private E-Mails im Mailaccount bzw am Firmenlaptop befinden.

Auch die Nutzung privater IT-Geräte wie Smartphones und Tablet-PCs für dienstliche Zwecke („*Bring your own device*“, kurz: BYOD) liegt nach wie vor im Trend. Neben dem

[1] Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

Vorteil, dass Mitarbeiter jederzeit von jedem Ort erreichbar sind und arbeiten können, bestehen etliche Gefahren, wie der Verlust oder Diebstahl der mobilen Endgeräte oder die Infizierung durch Schadsoftware, wodurch die über Synchronisierung mit dem Unternehmensnetzwerk mobil verarbeiteten Daten von Lieferanten, Kunden und dem Unternehmen selbst, gefährdet sind. Im Zusammenhang mit mobilen Endgeräten ist vor allem auf Sicherheitsrisiken und anwendbare Datensicherheitsmaßnahmen zu achten. Von großer Bedeutung sind jedoch auch die datenschutzrechtlichen Rahmenbedingungen bei der Kontrolle von Mitarbeitern. Soweit ersichtlich bestehen in Österreich für interne Kontroll- und Untersuchungsmaßnahmen keine expliziten Rechtsgrundlagen, weshalb die Anforderungen des Datenschutzrechts eingehalten werden müssen. Erhebliche Unklarheiten bestehen, wenn der Arbeitnehmer aus dem Unternehmen ausscheidet. Es stellt sich die Frage, ob der Arbeitgeber auf das mobile Endgerät nach Beendigung des Arbeitsverhältnisses zugreifen darf.

Da in diesen Fällen personenbezogene Daten im Arbeitsverhältnis verwendet werden, ist zu untersuchen, wie sich das Datenschutzrecht und das Arbeitsrecht zueinander verhalten. Neben dem datenschutzrechtlichen Schwerpunkt ist zunächst zu prüfen, ob private E-Mail- und Internetnutzung am Arbeitsplatz sowie BYOD zulässig sind, um anschließend die Kontrollmöglichkeiten des Arbeitgebers sowie die Sanktionen von Missbrauch im Detail darzustellen.

Ziel ist es, ein umfassendes Gesamtwerk über die rechtlichen Fragestellungen aus Arbeitsrecht, Datenschutz und Datensicherheit zu den bestehenden Rechtsproblemen im Umgang mit privaten Daten ausgeschiedener Arbeitnehmer zu erstellen.

2. Forschungsstand und Methodik

Zur Beantwortung der rechtlichen Fragestellungen wird eine Normen- und Judikaturanalyse durchgeführt. Über die private Nutzung von dienstlichen E-Mailadressen und Internet am Arbeitsplatz sowie zu BYOD und deren Kontrollmöglichkeiten gibt es keine konkreten gesetzlichen Bestimmungen und wenige Gerichtsentscheidungen. Die Frage, ob die private Nutzung von E-Mail und Internet trotz Verbot zulässig ist, wird in Anlehnung an die Judikatur zu Privattelefonaten am Arbeitsplatz beantwortet. Auch bei Fehlen einer entsprechenden Regelung im Unternehmen wird auf diese Judikatur zurückgegriffen. Hinsichtlich der Kontrolle von E-Mail und Internet bleibt ebenso auf Rechtsprechung abzuwarten. Soweit ersichtlich, hatten österreichische Gerichte noch über keine Streitigkeiten zwischen ausgeschiedenen Arbeitnehmern und Arbeitgeber über die private Nutzung des Mailaccounts zu entscheiden. Aus diesem Grund wird auf die Judikatur als auch Gesetzgebung in Deutschland Bezug genommen.

Weiters wird eine Sichtung der einschlägigen nationalen und internationalen Literatur vorgenommen. Dadurch wird der geltende Meinungsstand festgestellt, welcher anschließend kritisch analysiert wird. Beispielsweise besteht bei der Frage, ob im Falle der Verwendung privater Endgeräte für berufliche Zwecke der Arbeitnehmer als Betroffener, Dienstleister oder Auftraggeber iSd Datenschutzgesetzes anzusehen ist, noch kein einheitlicher Meinungsstand in der Literatur. An die Antwort dieser interessanten dogmatischen Frage knüpfen weitere Probleme etwa wie der Arbeitnehmer als datenschutzrechtlicher Dienstleister die Dienstleisterpflichten gemäß §§ 10, 11 Datenschutzgesetz 2000 (DSG 2000) erfüllen soll oder im Falle, dass der Arbeitnehmer als datenschutzrechtlicher Auftraggeber angesehen wird, der Arbeitgeber hinsichtlich der privaten Daten des Arbeitnehmers nicht den Bestimmungen zur Datensicherheit (§ 14 DSG 2000) unterliegt.

Betreffend der datenschutzrechtlichen Fragen wird darauf hingewiesen, dass auf die geplante Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) eingegangen wird. Zum Zeitpunkt der Erstellung des Exposés ist diese Verordnung jedoch noch nicht in Kraft.

3. Vorläufiges Inhaltsverzeichnis

I. Einleitung

II. Kontrollmöglichkeiten und -rechte des Arbeitgebers

1. E-Mail

1.1. Arbeitsrecht

1.1.1. Zulässigkeit aus individualarbeitsrechtlicher Sicht

a. Verbot der Privatnutzung

b. Keine Regelung über Privatnutzung

c. Erlaubnis der Privatnutzung

1.1.2. Zulässigkeit aus betriebsverfassungsrechtlicher Sicht

1.2. Datenschutz

1.2.1. Grundstruktur des DSG 2000

1.2.2. Begriffsbestimmungen

1.2.3. Rechtliche Anforderungen

1.2.4. Datenschutzrechtliche Zulässigkeitsprüfung der Kontrollmöglichkeiten des Arbeitgebers

a. Während dem bestehenden Arbeitsverhältnis

b. Nach Beendigung des Arbeitsverhältnisses

2. Internet

2.1. Arbeitsrecht

2.2. Datenschutz

3. Private Endgeräte (BYOD)

3.1. Definition

3.2. Arbeitsrecht

3.2.1. Individualvereinbarung

3.2.2. Betriebsvereinbarung

3.2.3. Kostentragung und Haftung

3.3. Datenschutz

3.3.1. Begriffsbestimmungen

3.3.2. Datenschutzrechtliche Zulässigkeitsprüfung des Zugriffes durch Arbeitgeber während dem bestehenden Arbeitsverhältnis

3.3.3. Datenschutzrechtliche Zulässigkeitsprüfung der Herausgabe der Unternehmensdaten nach Beendigung des Arbeitsverhältnisses

III. Strafbarkeit des Arbeitgebers und Sanktionen von Missbrauch

IV. Digitaler Nachlass – Rechtsprobleme im Zusammenhang mit dem Umgang mit elektronischen Daten nach dem Tod

V. Datensicherheit

1. Risiken und Gefahren
2. Haftung
3. Maßnahmen

VI. Conclusio

4. Zeitplan

Sommersemester 2012	VO Juristische Methodenlehre (2 SWS)
Wintersemester 2012/13	KU zur Judikatur- oder Textanalyse: System und wissenschaftliche Methode - Spinozas Ethik (2 SWS)
Wintersemester 2014/15	Themenfindung Einigung mit dem jetzigen Betreuer
Sommersemester 2015	Erstellung des Exposé Seminar aus Arbeits- u. Sozialrecht und Europarecht - für DissertantInnen zur Präsentation des Dissertations-vorhabens (2 SWS) Seminar aus Arbeitsrecht (2 SWS), Univ.-Prof. Dr. Brodil
Wintersemester 2015/16	Einreichung des Antrags auf Genehmigung des Dissertationsvorhabens Recherche und Verfassen der Dissertation unter regelmäßiger Rücksprache mit dem Betreuer Lehrveranstaltungen im Ausmaß von 4 SWS
Sommersemester 2016	Recherche und Verfassen der Dissertation unter regelmäßiger Rücksprache mit dem Betreuer Lehrveranstaltungen im Ausmaß von 2 SWS
Wintersemester 2016/17	Recherche und Verfassen der Dissertation unter regelmäßiger Rücksprache mit dem Betreuer Seminar im Ausmaß von 2 SWS
Sommersemester 2017	Korrektur und Überarbeitung der Dissertation
Wintersemester 2017/18	Abgabe der Dissertation und öffentliche Defensio

5. Vorläufiges Literaturverzeichnis

- *Beckschulze/Henke*, Der Einfluss des Internets auf das Arbeitsrecht, DB 2001, 1491
- *BITKOM*, Bring your own device, <www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf>
- *Brodil*, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 69
- *Brodil*, Arbeitsverhältnis, in: Studiengesellschaft für Wirtschaft und Recht (Hrsg), Geheimnisschutz – Informationsschutz – Datenschutz (2008)
- *Brodil*, Kontrolle und Datenschutz im Arbeitsrecht, ZAS 2009/21
- *Brodil/Risak/Wolf*, Arbeitsrecht in Grundzügen[8] (2013)
- *Däubler*, Internet und Arbeitsrecht² (2001)
- *Dohr/Pollirer/Weiss/Knyrim*, DSG. Kommentar Datenschutzrecht² (17. ErgLfg 2014)
- *Dürager*, Datenschutzrechtliche Aspekte der mobilen Kommunikation im Unternehmen: "Bring your own device" - ein Risiko für den Arbeitgeber?, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 137
- *Feiler*, Datenschutzrechtliche Herausforderungen bei internen Compliance-Untersuchungen, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2013 (2013) 143
- *Frank*, Bring your own device – Rechtliche und tatsächliche Aspekte, RDV 2013/4, 185
- *Goricnik/Riesenecker-Caba*, Datenschutz und Datensicherheit beim betrieblichen Einsatz mobiler "smarter" Endgeräte, Dako 2014/16, 34
- *B. Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in Österreichische Juristenkommission (Hrsg), Grundrechte in der Informationsgesellschaft (2001), 167
- *Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle (Wien 2014)
- *Huger/Laimer*, BYOD und Arbeitsrecht, ecolex 2014, 303
- *Jahnel*, Handbuch Datenschutzrecht (2010)
- *Jahnel/Mader/Staudegger*, IT-Recht³ (2012)
- *Kietaibl*, Arbeitsrecht 1. Gestalter und Gestaltungsmittel[8] (2013)
- *Knyrim*, Datenschutzrecht. Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm² (2012)

- *Knyrim/Horn*, Bring Your Own Device - Ein Trend hält Einzug in Österreichs Unternehmen, ecolex 2013, 365
- *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz. Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004/29, 167
- *Laimer/Mayr*, Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, DRdA 2003, 410.
- *Leissler*, BYOD und Datenschutz - ein unlösbarer Widerspruch?, ecolex 2014, 307
- *Obereder*, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, öRdA 2001, 75
- *Pollirer*, Checkliste - Bring Your Own Device (BYOD), Dako 2014/6, 12
- *Resch* (Hrsg), Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2006)
- *Schuster*, Bring Your Own Device! Zur Verwendung eigener Arbeitsmittel als Dienstnehmer, SWK 2012, 1065
- *Strasser/Jabornegg/Resch*, Kommentar zum Arbeitsverfassungsgesetz
- *Thiele*, Rechtssicherer Umgang mit elektronischen Accounts ausgeschiedener Mitarbeiter, jusIT 2014/1, 1
- *Tichy*, BYOD - Was steckt wirklich dahinter?, ecolex 2014, 300
- *Windisch-Altieri*, Von "Bring your OWN DEVICE" (BYOD) bis "Bring your own ANYthing" (BYOX). Nutzung privater Smartphones und Tablets im Büro - Risiken rechtlich absichern, AnwBl 2013, 467
- *Windisch-Graetz*, Arbeitsrecht 2. Sachprobleme[8] (2013)
- *Windisch-Graetz* in ZellKomm[2] (2011) § 1014 ABGB
- *Zankel*, Bring Your Own Device! Problemfelder der Übertragung von Arbeitgeberpflichten aus der Sicht des Arbeits- und des Datenschutzrechts, ASoK 2013, 423