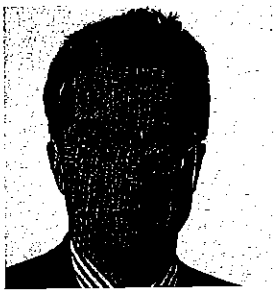
THOMAS HOEREN

BRING YOUR OWN DEVICE

RECHTLICHE FALLSTRICKE



Prof. Dr. Thomas Hoeren Jahrgang 1961. Von 1980 bis 1987 Studium der Theologie und Rechtswissenschaften, 1989 Promotion und 1994 Habilitation an der Universität Münster. 1995 bis 1997 Universitätsprofessor an der Juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf. Seit April 1997 Universitätsprofessor an der Juristischen Fakultät der Westfälischen Wilhelms-Universität Münster; Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM). E-Mail: hoeren@uni-muenster.de

Bring your own device (kurz BYOD) ist einer der großen Ttrends der letzten Jahre. Immer mehr Arbeitnehmer bringen ihre privaten Smartphones und Tablets mit ins Unternehmen und nutzen sie auch dienstlich. Zum Teil wird dies sogar von den Unternehmen erwartet und es sind eigene Infrastrukturen hierfür technisch vorgesehen. Im Folgenden sollen einige der wichtigsten juristischen Fallstricke bei BYOD aufgezeigt werden.

KEIN ZWANG

Ein Arbeitnehmer kann nicht dazu gezwungen werden, auf eigene Kosten einen Tablet oder ein Smartphone zu kaufen. Möglich ist jedoch, dies dienstlich zur Verfügung zu stellen. Eine Verpflichtung zur Nutzung ergibt sich dann aber auch nur insoweit, als der Arbeitnehmer darin einwilligt. Etwas anderes gilt, wenn Tablets oder Smartphones vom Arbeitgeber finanziert sind und deren Einsatz durch den Mitarbeiter dienstlich geboten ist (z. B. das Smartphone für Taxifahrer; der Tablet-PC für Außendienstmitarbeiter).

WEM GEHÖREN DIE DATEN?

Dann ist fraglich, wem die entsprechenden Daten auf den Geräten gehören. Dem Konzept des BYOD ist eine Gemengelage von dienstlicher und privater Datengenerierung immanent. Problematisch ist, dass das BGB ein Eigentumsrecht von Daten nicht kennt. Daten sind nicht eigentumsfähig, da sie keine beweglichen Sachen im Sinne von § 90 BGB sind. Allerdings setzt § 453 BGB eine entsprechende Anwendung des Kaufrechts auf solche Gegenstände voraus.[1] Zu bedenken ist zudem, dass nach dem Used-Soft-Fall beim Europäischen Gerichtshof von einer Veräußerung auch bei online erworbener Software ausgegangen werden muss.[2] Das Landesarbeitsgericht Chemnitz hat vertreten, dass die Eigentumsfrage u. a. durch Arbeitsverträge geregelt werden kann.[3] Ungeklärt ist dann aber, inwieweit eine Standardklausel zum Eigentumserwerb des Dienstherrn mit § 307 Abs. 1 BGB konform geht. Letztlich löst sich das Problem vertragsrechtlich, da aus § 667 BGB eine Pflicht zur Herausgabe der Daten bei dienstlichen Kontakten bestehen dürfte.

FERNÜBERWACHUNG – ZULÄSSIG?

Losgelöst von der Eigentumsfrage stellt sich das Problem, ob und inwieweit der Arbeitgeber Daten auf Smartphones und Tablets auslesen kann. Die Frage stellt sich insbesondere bei der Fernüberwachung solcher Geräte. Hier ist zwischen der privaten und der dienstlichen Nutzung zu unterscheiden. Wenn der Arbeitgeber überhaupt ein Zugriffsrecht hat, dann nur auf die dienstlichen Daten. Dies ergibt sich aus der Wertung des § 35 Abs. 3 BDSG. Dabei ist zu bedenken, dass selbst dann, wenn der Arbeitgeber die Nutzung der Geräte für rein dienstliche Zwecke vorgeschrieben hat, durch betriebliche Übungen private Nutzungsvorgänge legitimiert werden können. Bei einer solchen Verflechtung privater und dienstlicher Daten ist auch der Zugriff auf letztgenannte Datentypen rechtlich problematisch. Ein Vorgang, bei dem jedenfalls aufbewahrte Daten gelesen werden, wäre nach den Vorgaben des Telekommunikationsgeheimnisses (§ 88 TKG) verboten und über § 206 Abs. 1 StGB strafbar. Löscht der Arbeitgeber darüber hinaus sogar private Daten oder Mails, würde dies einen Schadensersatzanspruch nach § 280 Abs. 1 BGB bzw. § 823 Abs. 1 BGB auslösen. Hinzu kommt der Straftatbestand der Datenveränderung (§ 303a StGB).[4]

URHEBERRECHT – DARF DIE APP ÜBERHAUPT GENUTZT WERDEN?

Urheberrechtlich zu bedenkem ist, inwieweit die verwendete Software überhaupt für BYOD-Zwecke genutzt werden kann. In den Regularien zu Apps findet sich häufig der Zusatz, dass die App nur für den privaten Gebrauch eingesetzt werden darf. Wenn die App aber nun in einem dienstlichen Kontext zum

Tragen kommt, wäre dies eine Vertrags- und eine Urheberrechtsverletzung durch den Arbeitnehmer, für die der Arbeitgeber nach § 99 UrhG haftet. Ähnliches gilt für den Einsatz von Firmensoftware auf privaten Geräten, denn die Nutzung der Firmensoftware ist regelmäßig auf den gewerblichen oder dienstlichen Gebrauch beschränkt.

AUFBEWAHRUNGSPFLICHTEN – WAS WILL DAS FINANZAMT?

Als problematisch erweist sich ferner die Einhaltung von Aufbewahrungspflichten, etwa nach § 257 Abs. 1 HGB und § 147 AO. Auf dienstliche Daten muss das Finanzamt zugreifen können. Die Datenaufbewahrung muss also den Grundsätzen ordnungsgemäßer Speicherbuchführung entsprechen. Eine Löschung von dienstlichen Daten durch den Arbeitnehmer ist daher nicht erlaubt und würde zu Schadensersatzansprüchen nach § 280 Abs. 1 BGB und § 823 Abs. 1 BGB führen. Auch der Weiterverkauf des Smartphones oder des Tablets ist nur zulässig, sofern vorher die Daten dem Arbeitgeber zum Rücktransfer angeboten worden sind oder zumindest eine Sicherungskopie gemacht worden ist.

ES IST SONNTAG! ARBEITSZEITRECHTLICHE VORGABEN

Smartphones bringen eine enorme zeitliche Belastung für den Arbeitnehmer mit sich, der nunmehr auch an Wochenenden oder nach Feierabend für Geschäftspartner und Arbeitgeber erreichbar ist, sodass die gemäß § 3 ArbZG grundsätzlich geltende Arbeitszeit von täglich acht Stunden regelmäßig überschritten werden kann. Die Rufbereitschaft allein gilt nicht als Arbeitszeit, die zu vergüten wäre.[5] Nimmt der Arbeitnehmer den Anruf an, gilt dies ab diesem Moment als Arbeitszeit, die entsprechend zu vergüten ist.[6] Ferner verbietet § 10 Abs. 1 ArbZG den beruflichen Einsatz von Smartphones an Sonn- und Feiertagen. Hier sind technische Beschränkungen der Nutzung gemäß der arbeitszeitrechtlichen Vorgaben zwingend notwendig.

UND DER BETRIEBSRAT?

Der Einsatz von Smartphone und anderen BYOD-Geräten bedarf der Zustimmung des Betriebsrats. Denn all dies sind Geräte, die dazu geeignet sind, Verhalten und Leistung des Arbeitnehmers zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG).[7] Durch den Bezug zur Arbeitszeit und zu Überstundenfragen kommt auch eine Anwendung von § 87 Abs. 1 Nr. 2 und 3 BetrVG in Betracht.[8] Daher ist vor dem Einsatz solcher Geräte eine Betriebsvereinbarung aufzusetzen, die mit dem Betriebsrat/der Personalvertretung abgestimmt werden muss.[9]

WAS, WENN DAS HANDY BESCHÄDIGT WIRD?

Den Arbeitgeber treffen auch Ersatzpflichten bei Beschädigung des Smartphones, wenn dieses für Berufliches genutzt wird. Ihn trifft ein anteiliger Aufwendungsersatzanspruch nach § 670 BGB. Der Versuch, diesen Aufwendungsersatzanspruch durch allgemeine Geschäftsbedingungen/den Arbeitsvertrag auszuschließen, dürfte nach § 307 Abs. 1 BGB nichtig sein.[10] Im Übrigen besteht keine nebenvertragliche Pflicht des Arbeitnehmers, sich im Schadensfall ein neues Smartphone zu besorgen.

GEHEIM, GEHEIM, GEHEIM

Smartphones stellen außerdem ein Problem für den Geheimnisschutz dar. Viele Unternehmen sind entweder vertraglich oder gesetzlich zu besonderer Vertraulichkeit verpflichtet. Diese Geheimhaltung kann nur realisiert werden, wenn auch der Umgang mit Smartphones und Tablets durch eigene Geheimhaltungsrichtlinien geregelt wird. Diese Richtlinien müssen mit dem Betriebsrat abgestimmt werden. Dabei müssen sie vor allem auch eine Kontrolle der Einhaltung von Datensicherheitsstandards und deren Sanktionierung vorsehen. Wichtig ist auch, dass ein Verbot des Einsatzes sicherheitsrelevanter Apps sowie der freie Weiterverkauf solcher Geräte oder die Abgabe an Kinder und sonstige Unberechtigte festgeschrieben ist.

VORSICHT!

Wer Dritten seine Kontaktdaten mitteilt, gibt ein Signal, dass er für sie jederzeit erreichbar ist. Dies kann dazu führen, dass besondere Sorgfaltspflichten im Umgang mit Kunden und Mandanten entstehen. Die Rechtsprechung ging bisher davon aus, dass derjenige, der seine E-Mail-Adresse geschäftlich bekannt gibt, auch für eine entsprechend schnelle Antwort vorsorgen muss.[11] Es hilft dabei nicht, sich durch sogenannte Disclaimer (in Form von automatisierten Rück-E-Mails) von der Verantwortlichkeit freizuzeichnen. Als besonders gefährlich erweist sich das Smartphone-Tool WhatsApp, da dort Nachrichten als markiert gelesen werden und diese Funktionalität nur bei wenigen Betriebssystemen, wie z.B. bei iOS, nicht aber bei Android, abgestellt werden kann.

BRING YOUR OWN ACCOUNT!?

Ähnlich problematisch wie BYOD ist auch das immer mal wieder geforderte »Bring your own account«. Die rechtliche Einordnung von Accounts ist noch völlig ungeklärt. Unklar ist daher auch, wem ein Account gehört und in welchen Fällen man von einem dienstlichen oder privaten Account ausgehen kann und muss. In besonderer Weise macht sich dieses Problem bemerkbar, wenn der Accountinhaber stirbt. In diesem Fall werden verschiedene Lösungen in der Literatur vertreten, von der Übertragung der Accountrechte an Angehörige, den Erben oder im beruflichen Fall dem Arbeitgeber.

FAZIT

Möchte ein Unternehmen BYOD im Betrieb zulassen, so sollte es dafür sorgen, dass in allen genannten Bereichen Regelungen zum Teil unter Mitwirkung des Betriebsrats getroffen werden. Dabei geht es im Wesentlichen um zwei Bereiche. Im Arbeitsvertrag ist die Einwilligung des Arbeitnehmers zur teilweise dienstlichen Nutzung seiner privaten Geräte zu regeln. Hinzu kommt eine Betriebsvereinbarung mit einer Zusatzvereinbarung für die Geheimhaltung.

1 *Jickeli/Stieper* in Staudinger, § 90 BGB Rn. 17.
2 EuGH, Urt. v. 3.7.2012 – C-128/11 NJW 2012, 2565 = GRUR 2012, 904 = EuZW 2012, 658 – UsedSoft.
3 LAG Chemnitz, Urt. v. 17.01.2007 – 2 Sa 808/05.
4 *Göpfert/Wilke*, NZA 2012, 767.
5 BAG, Urt. v. 11.7.2006 – 9 AZR 519/05, NZA 2007, 155 = BB 2007, 272.
6 *Steinau-Steinrück*, NJW-Spezial 2012, 179.
7 ArbG Frankfurt a. M., Beschl. v. 20.1.2004 – 5 BVGa 14/04, MMR 2004, 344.
8 *Falder*, NZA 2010, 1154.
9 *Arning, Moos, Becker*, CR 2012, 593.
10 BAG, Urt. v. 21.6.2011 – 9 AZR 203/10, NJW 2012, 106 = NZW 2011, 1338.
11 EuGH, Urt. v. 16.10.2008 – C-298/07, EuZW 2008, 692 = NJW 2008, 3553.