RICHTERLICHE UNABHÄNGIGKEIT UND BRING YOUR OWN DEVICE (BYOD) – WEG IN DIE ZUKUNFT ODER UNVERTRETBARES SICHERHEITSRISIKO?

Jochen Krüger / Frederik Möllers / Stephanie Vogelgesang

Vizepräsident des Amtsgerichts Saarbrücken a.D. und wissenschaftlicher Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
66123 Saarbrücken, DE
jochen.krueger@uni-saarland.de

Wissenschaftlicher Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA an der Universität des Saarlandes
66123 Saarbrücken, DE
frederik.moellers@uni-saarland.de

Wissenschaftliche Mitarbeiterin, juris-Stiftungsprofessur für Rechtsinformatik und CISPA an der Universität des Saarlandes
66123 Saarbrücken, DE
stephanie.vogelgesang@uni-saarland.de

Schlagworte: ***Richterliche Unabhängigkeit, elektronische Akte (E-Akte), elektronische Aktenführung, Bring Your Own Device (BYOD), private Mobilgeräte, Datenschutz, Sicherheitsrisiken, Sandboxes***

Abstract: *Die richterliche Unabhängigkeit gehört zu den zentralen Gestaltungsgrundsätzen für die Justiz. Das Konzept «Bring Your Own Device» (BYOD), also die Nutzung privater Mobilgeräte zu dienstlichen Zwecken, ist eine der neuen Entwicklungstendenzen in der digital geprägten Arbeitswelt. Die dadurch eröffnete Möglichkeit, an jedem Ort und zu jeder Zeit zu arbeiten, kommt auch dem Selbstverständnis der Richter entgegen. Der Beitrag erörtert die Frage, ob BYOD bei Richtern ein zukunftsweisendes Modell darstellt oder ob unter technischen und datenschutzrechtlichen Aspekten gravierende Sicherheitsrisiken bestehen.*

1. Allgemeine Problemstellung

Durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERV-Gesetz oder eJustice-Gesetz) vom 10. Oktober 2013 ist die Entwicklung in der Justiz zur elektronischen Aktenführung in Deutschland vorgezeichnet.[1] Im Entwurf zur Einführung der E-Akte im Strafverfahren[2] ist nunmehr auch ab dem 1. Januar 2026 eine entsprechende Pflicht für neu angelegte Strafakten vorgesehen. Dabei sind auch neue technische Entwicklungen auf ihre Verwendbarkeit für die Justiz zu prüfen.[3] Auf diesem Hintergrund soll im Folgenden das Konzept «Bring Your Own Device» (BYOD) im Zusammenhang mit Fragen der richterlichen Unabhängigkeit erörtert werden. Dafür sind zunächst die prägenden Grundgedanken beider Bereiche zu skizzieren.

1.1. Zum Grundgedanken der richterlichen Unabhängigkeit

Die richterliche Unabhängigkeit (Art. 97 GG) gehört in Deutschland zu den traditionellen zentralen Gestaltungsgrundsätzen für die Justiz, die auch im Rahmen der elektronischen Aktenführung zu berücksichtigen

1 Vgl. Müller, eJustice – Die Justiz wird digital, JuS 2015, S. 609.

2 Vgl. Art. 21 Abs. 6 Nr. 1 Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 6. Mai 2016, BR-Drucksache 236/16.

3 Vgl. Thesenpapier des Deutschen Richterbundes zum Richter- und Staatsanwaltsarbeitsplatz (April 2014) unter 2.

sind.[4] Gemäß Art. 92 GG ist die rechtsprechende Gewalt den Richtern[5] vorbehalten. Gemäß Art. 97 Abs. 1 GG sind Richter unabhängig und nur dem Gesetz unterworfen. Gleichzeitig ist jedoch offensichtlich, dass Richter nicht autark arbeiten. Sie bedürfen bei ihrer Arbeit sachlicher und organisatorischer Unterstützung. Verboten ist – nur – die inhaltliche Einflussnahme von außen.[6] Dabei schützt der Grundsatz der richterlichen Unabhängigkeit bereits vor jeder vermeidbaren – auch subtilen oder psychologischen – Einflussnahme der Exekutive auf die Rechtsentscheidung.[7]

1.2. Zum Grundkonzept des BYOD

Das Konzept BYOD, also die Nutzung privater Mobilgeräte für dienstliche Zwecke, ist eine der Entwicklungstendenzen in der neueren Arbeitswelt. Dies gilt nicht nur für Deutschland,[8] sondern weltweit.[9] Allgemein entspricht der Gedanke der Consumerisation, also der Aufhebung der Grenzen privater und dienstlicher Tätigkeit,[10] offensichtlich dem Zeitgeist. BYOD ist eng verbunden mit dem Stichwort Arbeiten 4.0.[11] Dieser Ansatz ist u. a. gekennzeichnet durch einen verstärkten Wunsch nach Arbeitszeitsouveränität. Insbesondere eröffnet BYOD auch die Möglichkeit einer Heimarbeit.

Beim Konzept BYOD gehört dem Arbeitnehmer das eingesetzte Endgerät. In der Regel handelt es sich dabei um ein privates Tablet, ein Smartphone oder ein Notebook.

BYOD bedeutet damit für den Arbeitnehmer eine größere Wahlfreiheit. Persönliche Bedürfnisse können besser berücksichtigt werden. Dies führt typischerweise zu einer größeren Zufriedenheit und damit auch letztlich zu einer höheren Arbeitseffizienz. Zudem haben die vom Arbeitnehmer privat besorgten Geräte oftmals einen höheren technischen Standard als die Geräte, die im Rahmen der allgemeinen Firmenorganisation normalerweise vorgehalten werden.[12] Daher liegt der Ansatz nahe, den Gedanken der richterlichen Unabhängigkeit mit dem Konzept BYOD zu koppeln.

2. BYOD und richterliche Unabhängigkeit

2.1. Anmerkungen zum allgemeinen Diskussionsstand

BYOD wird mit Blick auf die freie Wirtschaft relativ umfangreich diskutiert.[13] Das Thema «staatliche Behörden und BYOD» wird in Deutschland dagegen nur zögerlich aufgenommen. Der IT-Planungsrat hat ausweislich einer Mitteilung des Bundesministeriums des Innern vom 26. Juni 2015[14] mit Beschluss 2015/25 nunmehr eine offene Arbeitsgruppe BYOD eingerichtet. Ziel ist es, Wege aufzuzeigen, unter welchen Rahmenbedingungen der Einsatz privater mobiler Endgeräte u.a. in der Verwaltung sinnvoll sein kann. Auch das Arbeitspapier der International Working Group on Data Protection in Telecommunications (Sitzung 14./15. Oktober 2014 in

4 Vgl. dazu und zum Folgenden Berlit, Richterliche Unabhängigkeit und Elektronische Akte, JurPC Web-Dok 77/2012, Abs. 1 ff.

5 Im Folgenden sind sowohl Richterinnen als auch Richter gemeint; allgemein wird zur Vereinfachung der Darstellung die männliche Form gewählt.

6 Zu den damit verbundenen Grundsatzproblemen Berlit (Fn. 4), Abs. 14 ff.

7 Radke, Datenhaltung und Datenadministration der Justiz und richterliche Unabhängigkeit, jM 2016, S. 9 m.w.N.

8 Vgl. dazu zusammenfassend Heldmann, Dienstliche Nutzung privater Endgeräte (BYOD) und privater Gebrauch dienstlicher Kommunikationsmittel, 2015.

9 French/Guo/Shim, Current Status, Issues, and Future of Bring Your Own Device (BYOD), in Communications of the Association for Information Systems, 2014, Vol. 35, Article 10.

10 Vgl. dazu Bundesamts für Sicherheit in der Informationstechnik (BSI), Überblickspapier Consumerisation und BYOD, 31. Juli 2013.

11 Vgl. dazu Bissels/Meyer-Michaelis, Arbeiten 4.0 – Arbeitsrechtliche Aspekte einer zeitlich-örtlichen Entgrenzung der Tätigkeit, DB 2015, S. 2331 ff.

12 Vgl. dazu Heldmann (Fn. 8), S. 8.

13 Vgl. z.B. die Literaturübersicht bei Heldmann (Fn. 8).

14 Bundesministerium der Innern (BMI), Bekanntmachung Entscheidungen des IT-Planungsrats, 26. Juni 2015.

Berlin)[15] zum Konzept BYOD erörtert zwar die offiziellen Auffassungen zu BYOD bei staatlichen Behörden, z.B. in den USA, in England und Frankreich. Für Deutschland wird auf das «Überblickspapier Consumerisation und BYOD» des BSI verwiesen. Dieses befasst sich jedoch nicht näher mit der Justiz. Das Thema BYOD und Justiz war dagegen Gegenstand auf dem EDV-Gerichtstag 2013 in Saarbrücken.

2.2. Besonderheiten beim Thema «Richterliche Unabhängigkeit und BYOD»

Im vorliegenden Beitrag steht das Thema BYOD und richterliche Unabhängigkeit im Mittelpunkt.[16] Dies muss betont werden. Denn diese Thematik weist bei näherer Analyse faktische, strukturelle und rechtstheoretische Besonderheiten gegenüber der «Normaldiskussion» um BYOD in der digitalen Arbeitswelt auf.

Einige Gesichtspunkte sollen im Folgenden skizziert werden.

1. Bei Richtern ist anerkannt, dass sie ihre Arbeitszeit und ihren Arbeitsort grds. frei wählen können, wenn nicht aus sachlichen Gründen – wie z.B. Durchführung von Gerichtsverhandlungen – die Anwesenheit bei Gericht erforderlich ist. Richter sind auch nach eigenem Selbstverständnis geborene Heimarbeiter und erledigen einen Großteil ihrer Aufgaben zu Hause. Heimarbeit hat daher für Richter – auch unter dem Gesichtspunkt der Vereinbarkeit von Beruf und Familie – eine hohe Akzeptanz und beruht auf dem Grundgedanken der Freiwilligkeit. Das in der allgemeinen Diskussion erörterte Problem, ob BYOD vom Unternehmen zwangsweise angeordnet werden kann,[17] spielt im Zusammenhang mit Richtern nur eine untergeordnete Rolle.
2. Bei Richtern entfallen im Ansatz auch einige technokratische Einzelfragen, die sonst als Probleme erörtert werden. Die gilt z.B. für die Frage, ob die Heimarbeit als Arbeitszeit gewertet werden muss. Fragen der allgemeinen Rufbereitschaft als Arbeitszeit und die damit verbundene Frage von Regelarbeitszeiten sind bei richterlicher Arbeit ebenfalls kein Grundsatzproblem.
3. Allgemein sind Richter keine Arbeitnehmer im klassischen Sinne. Insbesondere fehlt es an der durchgängigen Weisungsabhängigkeit, die sonst ein Arbeitsverhältnis charakterisiert. Daher können auch für das Arbeitsverhältnis selbstverständliche Anweisungs- und Kontrollmechanismen nur bedingt gegenüber Richtern eingesetzt werden. Dass daraus gerade für die vorliegende Problematik neue Fragen entstehen können, werden die folgenden Ausführungen zeigen.

2.3. Richterliche Unabhängigkeit in Zeiten der E-Akte

Die Konturen der richterlichen Unabhängigkeit wurden auf dem geistigen Hintergrund der Papier-Akte entwickelt. Dadurch erhält die hier gewählte Thematik eine zusätzliche Akzentsetzung. Denn nach Einführung der E-Akte muss der Gedanke der richterlichen Unabhängigkeit allgemein neu justiert werden.[18] Einschlägige Gerichtsentscheidungen machen dabei deutlich,[19] dass die Digitalisierung der Justiz teilweise als Beschränkung und Bedrohung der richterlichen Unabhängigkeit empfunden wurde. So wurde gerügt, dass der Einsatz von Technik eine externe Kontrolle richterlicher Tätigkeit eröffnet, die qualitativ und quantitativ die bisherigen Möglichkeiten der Dienstaufsicht weit überschreitet.[20] Bei der elektronischen Aktenführung kann im Verhältnis zur Papier-Akte auf Daten in größerem Umfang, innerhalb kürzerer Zeit, bei zentralem IT-Einsatz durch einen erweiterten Kreis von Zugangsberechtigten und in der Regel unbemerkt zugegriffen werden. Bundes-

[15] Abrufbar unter: https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group/ (alle Websites zuletzt abgerufen am 1. Februar 2017).

[16] Vgl. dazu auch Berlit, Der Richter als Sicherheitsrisiko? Richterliche Unabhängigkeit und IT-Sicherheit, jM 2016, S. 334.

[17] Vgl. dazu und zum Folgenden Heldmann (Fn. 8), S. 52 f.

[18] Vgl. dazu insbesondere Berlit (Fn. 4), Abs. 28 ff.

[19] Vgl. dazu und zum Folgenden Krüger/Möllers, Metadaten in Justiz und Verwaltung, MMR 2016, S. 729 f.

[20] Vgl. in diesem Zusammenhang BVerfG, Beschluss vom 17. Januar 2013, NJW 2013, 2102.

weites Aufsehen hat auch die Klage eines Registerrichters erweckt. Dieser hatte – im Ergebnis erfolglos[21] – verlangt, dass die digitalen Eingänge zum Handelsregister für ihn zwecks leichterer Bearbeitung ausgedruckt werden.

2.4. Richterliche Unabhängigkeit und BYOD – eine potentielle Idealkombination

Die Einführung von BYOD bei Richtern könnte demgegenüber positive Akzente setzen und die Akzeptanz der E-Akte fördern. BYOD ermöglicht bei digitaler Aktenführung eine vom Benutzer erwünschte Heimarbeit. Der Gedanke der richterlichen Unabhängigkeit kann dabei als rechtstheoretische Grundlage, jedenfalls als geistiger Motor[22] dieser Entwicklung herangezogen werden. Unter diesem Aspekt wäre die geistige Verbindung von richterlicher Unabhängigkeit und BYOD geradezu eine zukunftsweisende Traumkombination von traditionellem Rechtsgrundsatz und moderner Informationstechnik. Dies hätte auch unmittelbare Vorteile für die Justiz insgesamt. Allgemein gibt es einen verstärkten Konkurrenzkampf um kluge Köpfe mit IT-Kenntnissen. Der Leitfaden des IT-Planungsrats vom 16. Juni 2016 «IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln» befasst sich genau mit dieser Problematik. Einem vergleichbaren Kampf um ein positives Arbeitgeberimage wird sich auch die Justiz stellen müssen.[23] Die Einführung von BYOD könnte dabei helfen. Gerade für junge Menschen ist die Nutzung von eigenen Geräten für private und dienstliche Zwecke ganz überwiegend selbstverständlich.[24]

3. Technische Grundsatzfragen

Ein solches Konzept erfordert aber, dass bei der Umsetzung die Datenschutz- und Sicherheitsstandards eingehalten werden können, die für die Justizarbeit in digitalen Zeiten gelten. Dazu gehört, dass aktuelle Maßnahmen zum Schutz vor Schadsoftware Anwendung finden.[25] Auch müssen dienstliche und private Daten auf dem eingesetzten Mobilgerät getrennt werden.

3.1. Allgemeine Herausforderungen

Im Folgenden werden einige grds. Herausforderungen des Konzepts BYOD beleuchtet und potentielle Lösungsmöglichkeiten erörtert.

3.1.1. Schutz des gerichtsinternen Netzes

Eine offensichtliche Herausforderung stellt die Tatsache dar, dass bei BYOD ein privates Gerät Zugang zum gerichtsinternen Netz erhalten muss. Die Verfügung über das mobile Gerät hat einzig und allein der Besitzer selbst. Auf die Auswahl der installierten Software bzw. der ausgeführten Aktivitäten hat das Gericht oder dessen IT-Verwaltung nur geringen Einfluss. Eine klare Definition der Schnittstellen und Berechtigungen wird somit zu einem essentiellen Bestandteil des Konzepts BYOD. Wird das Privatgerät des Richters bspw. mit Malware infiziert, muss die Verbreitung im Netzwerk des Gerichts verhindert werden. Gleiches gilt für den unberechtigten Zugriff auf gerichtsinterne Daten. In der Praxis sind also die Privatgeräte als «nicht vertrauenswürdig» einzustufen. Daher müssen entsprechende Schutzmaßnahmen wie Firewalls zwischen ihnen und dem vertrauenswürdigen, gerichtsinternen Netz installiert werden.[26]

---

21 Vgl. BGH, Urteil vom 21. Oktober 2010, RiZ(R) 5/09 und dazu Brosch, Urteilsanmerkung zu: Bundesgerichtshof, Urteil vom 21. Oktober 2010, RiZ(R) 5/09 (1), JurPC Web-Dok. 1/2011, Abs. 1 ff.

22 Vgl. Berlit (Fn. 4), Abs. 53.

23 Vgl. Müller (Fn. 1), S. 613.

24 Vgl. Miller/Voas/Hurlburt, BYOD: Security and Privacy Considerations, IT Pro September/October 2012, S. 53.

25 BSI (Fn. 10), S. 7.

26 Vgl. Bundesamts für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kataloge, 15. Ergänzungslieferung, 2016, S. 4367 f.

3.1.2. Schutz der Geräte

Ebenso wichtig ist auch der Schutz der Geräte selbst. Aufgrund der nicht vorhandenen Kontrolle des Arbeitgebers über die privaten Geräte kann dieser hier nur wenige technische Sicherheitsmaßnahmen einsetzen. Das Hauptaugenmerk muss daher auf Unterstützung und Schulung liegen. Auch allgemeine Vorgaben oder Regeln lassen sich prinzipiell etablieren. Diese müssen jedoch auch auf Akzeptanz stoßen.

Zu möglichen technischen Maßnahmen zählt etwa die Bereitstellung von Software durch den Arbeitgeber selbst. Es liegt im Interesse des Arbeitgebers, dass die Nutzer auf ihren Geräten effektive Antivirensoftware sowie Software zur Nutzung der Schnittstellen zum Gericht (z.B. einen VPN-Client) einsetzen. Die Bereitstellung durch den Arbeitgeber ermöglicht es ihm außerdem, Updates zeitnah verfügbar zu machen und die Nutzer über diese zu informieren.

Bereits diese Hinweise konkretisieren aber auch das zu erwartende Problemfeld. So stellt sich im Ansatz die Frage, ob der Arbeitgeber für jedes denkbare Gerät eine effektive Anti-Viren-Software anbieten kann. Entschieden werden muss auch, wer die Kosten für das vom Arbeitgeber angebotene Programm tragen soll. Letztlich muss die Zentralfrage entschieden werden – was geschieht, wenn der richterliche Nutzer ein Update durch den Arbeitgeber ablehnt und dieses selbst durchführen will. Für diese Ablehnung kann es zahlreiche Gründe geben (z.B. Kostengesichtspunkte, Qualitätsanforderungen, nicht genügend gerichtliche Kapazität für das sofortige Aufspielen eines Updates).

3.2. (Temporäre) Speicherung der Daten auf dem Endgerät

Eine für den Nutzer komfortable Möglichkeit, das Konzept BYOD umzusetzen, besteht in der Speicherung dienstlicher Daten auf seinem Endgerät.

3.2.1. Auswahl der Dokumente bei Gericht

Der Arbeitsablauf könnte sich dann wie folgt gestalten: Im Gericht trifft der Richter eine Auswahl der Dokumente, an denen er unterwegs oder zu Hause arbeiten möchte. Diese werden auf sein Gerät übertragen und stehen dort zur Verfügung. Für den Zugriff außerhalb des Gebäudes benötigt er keine zusätzliche Software und keine bestehende Internetverbindung.

Dieser Ansatz hat eine erkennbare Schwachstelle. Der Richter muss sich bereits im Gericht entscheiden, mit welchen Dokumenten genau er später arbeiten will. Dies wird den praktischen Anforderungen nicht gerecht. Typischerweise merkt ein Bearbeiter erst bei der konkreten Befassung mit einem Problem, welche Daten er im Einzelnen für seine Entscheidung braucht.

3.2.2. Herunterladen der Dokumente mit Hilfe eines VPN-Client

Diesem Einwand könnte wie folgt Rechnung getragen werden. Der Richter kann von außerhalb Dokumente bei Bedarf etwa mit Hilfe eines VPN-Clients aus dem Gericht herunterladen und diese dann am privaten Rechner bearbeiten. Dies setzt zumindest für den Vorgang der Übertragung eine bestehende Internetverbindung zum Gericht voraus. Da die Daten dann aber persistent auf dem mobilen Endgerät gespeichert sind, kann der Richter fortan ohne bestehende Verbindung an diesen arbeiten.

Die VPN-Schnittstelle bietet zwar für den Richter einen erhöhten Komfort, birgt jedoch auch neue Gefahren. Sie muss über das Internet global erreichbar sein, damit der Richter seinen Arbeitsort frei wählen kann. Folglich haben jedoch auch Kriminelle die Möglichkeit, die Schnittstelle anzugreifen. Wird eine solche Schnittstelle also angeboten, muss sie durch entsprechende Maßnahmen (z.B. Intrusion-Detection-Systeme und geeignete Authentifizierungsmechanismen) gesichert sein.

3.2.3. Synchronisierung und Änderungsverfolgung

Unabhängig davon, ob Dokumente nur vor Ort oder auch mit Hilfe einer Fernzugriffssoftware auf das Gerät des Richters übertragen werden, stellt sich bei der Rückkehr an das Gericht das Problem der Synchronisierung.

Änderungen, die der Richter an den Dokumenten vorgenommen hat, müssen in das gerichtsinterne Netz übertragen werden. Dabei dürfen Änderungen, die bspw. in der Zwischenzeit von anderen Personen vorgenommen wurden, jedoch nicht verloren gehen.

Dieses Problem findet sich in vielen Bereichen der digitalen Arbeit. Erste Ansätze wurden bereits in den Siebzigerjahren diskutiert.[27] Auch für die Verwaltung moderner Office-Dokumente gibt es effektive Systeme zur Versionsverwaltung.[28] Diese Problematik kann daher auch ohne Einzelanalyse als prinzipiell lösbar eingestuft werden.

3.2.4. Sandboxing

Um Malware und unautorisierten Dritten den Zugriff auf dienstliche Daten verwehren zu können, müssen diese von den privat vorgehaltenen Daten und Anwendungen getrennt werden. Hierzu bieten sich verschiedene Ansätze an, die unter dem Begriff Sandboxing zusammengefasst werden können. Insbesondere bei den Betriebssystemen heutiger Smartphones wie z.B. Android oder iOS findet Sandboxing Anwendung.[29] Verschiedene Apps laufen strikt voneinander getrennt und können nur dann Daten austauschen, wenn dies von beiden Anwendungen vorgesehen und unterstützt wird. Das Betriebssystem übernimmt die Aufgabe, den gegenseitigen Zugriff zu kontrollieren.

Auf dem PC kommen insbesondere drei Maßnahmen in Betracht:

Virtualisierungslösungen bieten einen hohen Schutz für die Daten auf dem Wirtssystem. Das Gast-system kann nicht darauf zugreifen und lässt sich somit beliebig nutzen. In der Praxis ist der Ansatz jedoch wenig praktikabel: Speichert der Richter dienstliche Daten in einer virtuellen Maschine, so sind sie nicht ausreichend vor einem Zugriff über das private Wirtssystem geschützt. Jeder mit Zu-griff auf das Gerät kann die virtuelle Maschine manipulieren. Zwar könnte der Richter private Daten in einer virtuellen Maschine speichern und das Wirtssystem für die Arbeit nutzen. Diese Alternative ist wegen der geringen Bedienerfreundlichkeit jedoch wenig attraktiv. Aus diesen Gründen scheiden Virtualisierungslösungen als praktikable Maßnahme zum Schutz der Daten aus.

Eine andere Möglichkeit besteht darin, verschiedene Betriebssysteme nebeneinander auf demselben Gerät zu installieren. Verschlüsselt man zusätzlich die jeweiligen Systeme mit Hilfe entsprechender Software (bspw. BitLocker, VeraCrypt oder LUKS), so sind die Daten des dienstlich genutzten Systems selbst bei einer vollständigen Kompromittierung des privat genutzten Systems noch geschützt. Des Weiteren kann feingranular festgelegt werden, inwieweit der Dienstherr das dienstlich genutzte System bereitstellt und/oder administrieren kann. Die private Nutzung bleibt davon unbeeinflusst. Einziger Nachteil des Ansatzes ist der Aufwand, beim Übergang zwischen privater und dienstlicher Nutzung das Betriebssystem zu wechseln.

Der dritte Ansatz nutzt die vorhandenen Mittel des installierten Betriebssystems. Teilt man die Daten auf verschiedene Benutzeraccounts auf (z.B. einen dienstlichen und einen privaten), kann bereits das Betriebssystem den Zugriff eines im privaten Kontext gestarteten Programms auf dienstliche Daten unterbinden. Durch die Wahl verschiedener Passwörter können bspw. auch Familienmitglieder oder Diebe nicht sofort auf dienstliche Daten zugreifen. Setzt man zusätzlich Verschlüsselungssoftware ein, verringert sich auch das Risiko einer Kompromittierung weiter. Ein Restrisiko besteht allerdings durch sogenannte Privilege-Escalation-Sicherheitslücken, welche die Schutzmaßnahmen des Betriebssystems außer Kraft setzen.

---

[27] Vgl. Rochkind, The source code control system, IEEE Transactions on Software Engineering 4/1975, S. 364 ff.

[28] Vgl. Rönnau/Scheffczyk/Borghoff, Towards XML version control of office documents, Proceedings of the 2005 ACM symposium on Document engineering, S. 10 ff.

[29] Vgl. Android Developers, Security Tips, https://developer.android.com/training/articles/security-tips.html und Apple Developers, About App Sandbox, https://developer.apple.com/library/content/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html.

3.3. Keine Vorhaltung der Daten auf dem Endgerät

Insbesondere bei IT-Unternehmen findet sich häufig der Ansatz, dienstliche Daten gar nicht erst auf den Endgeräten der Arbeitnehmer zu speichern. Stattdessen werden die Daten in der Dienststelle auf einem Server oder dem Arbeitsplatzrechner des Nutzers vorgehalten. Am Arbeitsplatz kann letzterer dann über das Intranet (d.h. Netzwerkkabel oder WLAN) auf diese zugreifen. Eine moderne Netzwerkinfrastruktur ermöglicht komfortablen Zugriff ohne wahrnehmbare Verzögerungen und erlaubt unterbrechungsfreies Arbeiten.

Das Konzept lässt sich auch auf die Justiz übertragen: Die Daten werden dann auf einem Server bei Gericht oder im geschützten Netz der Justiz gespeichert. Vor Ort können die Richter sowohl mit ihrem Arbeitsplatzrechner als auch mit ihrem eigenen Gerät über das lokale Netz darauf zugreifen. Die Daten verlassen dabei niemals das Netzwerk des Gerichts.

Für die Heimarbeit oder die Arbeit unterwegs ist eine entsprechende Schnittstelle notwendig, um den Zugriff auf die Daten im internen Netzwerk zu ermöglichen. Dies könnte bspw. durch eine Remote-Desktop-Verbindung über ein VPN realisiert werden. Notwendig ist in jedem Fall eine Authentifizierung, so dass Unbefugten der Zugriff verwehrt werden kann.

Der Verlust oder Diebstahl des Endgeräts bzw. dessen Weitergabe an Dritte führt nicht notwendigerweise zur Kompromittierung der Sicherheit, sofern die Zugangsdaten weiterhin ausschließlich dem Richter selbst bekannt sind.

Dennoch stellen sich auch hier einige grundlegende Herausforderungen. Dies gilt insbesondere für die Verbindung zum Server. Wird diese unterbrochen, so kann der Richter nicht länger auf die Daten zugreifen und muss bis zur Wiederherstellung der Verbindung warten. Um das Problem zu umgehen, müssen die Daten wie in der zuvor beschriebenen Alternative auf dem Mobilgerät des Richters zwischengespeichert werden. Dies bringt jedoch auch die damit verbundenen Probleme mit sich. Auch die Sicherheit der Schnittstelle muss – wie oben beschrieben – gewährleistet sein, um Außenstehenden den Zugang zu vertraulichen Daten nicht zu ermöglichen.

Als Zentralproblem erweist sich aber der Schutz vor Malware. Erlangt ein Angreifer unbemerkt Kontrolle über das verbundene Endgerät, bekommt er Zugang zu denselben Daten wie der Richter auch.

4. Rechtliche Grundsatzfragen

Die bisherigen Erfahrungen mit BYOD weisen darauf hin, dass allgemein der Nutzer die theoretische und praktische Schwachstelle des Sicherheitskonzepts darstellt.[30] Dies gilt auch unter rechtlichen, insbesondere datenschutzrechtlichen, Aspekten.

4.1. Zur Bedeutung des Eigentums am Endgerät

Insbesondere ist der in der Diskussion um BYOD oft unterschätzte Gesichtspunkt zu beachten, dass das eingesetzte Endgerät im Eigentum des Nutzers bleibt. Dieses Eigentumsrecht gibt rechtstheoretisch die Möglichkeit, z.B. das Gerät zu jeder Zeit zu verkaufen, zu verschenken oder anderen zur Benutzung zu überlassen. Nach der bei Heldmann[31] abgedruckten Musternutzungsvereinbarung darf das private mobile Endgerät ausschließlich durch den Mitarbeiter genutzt werden (Regelung 3.4). Dies erledigt zwar ein Teilproblem, ist in der Sache aber eine weitgehende Aufgabe des Konzepts BYOD. Denn dieses ist durch das Eigentumsrecht des Nutzers am Endgerät geprägt, das auch die Weitergabe an Dritte beinhaltet. Einen Verkauf des Privatgeräts kann der Arbeitgeber bereits aus eigentumsrechtlichen Erwägungen nicht verhindern. Hierbei dürfen jedoch keine dienstlichen Daten in die Hände Dritter gelangen. Daher spielen Datenträgerverschlüsselung sowie das sichere

[30] Vgl. Disterer/Kleiner, BYOD – Bring Your Own Device, HMD – Praxis der Wirtschaftsinformatik 50 (2013), 290, S. 100.
[31] Heldmann (Fn. 8), S. 112.

Löschen von Daten vor einem Verkauf eine zentrale Rolle in möglichen Vereinbarungen zwischen Arbeitnehmer und Arbeitgeber.

4.2. Zur datenschutzrechtlichen Verantwortlichkeit des Arbeitgebers

Im Konzept BYOD bleibt die Verantwortlichkeit des Arbeitgebers für die Einhaltung der datenschutzrechtlichen Bestimmungen bestehen.[32] Dies gilt auch bei Richtern. Die jeweiligen Gerichte sind weiterhin verantwortliche Stelle bei der Bearbeitung von personenbezogenen Daten i.S.d. § 3 Abs. 7 BDSG. Damit haben sie auch die erforderlichen technischen und organisatorischen Maßnahmen i.S.d. § 9 BDSG bzw. der jeweiligen Landesdatenschutzgesetze zu treffen. Bei Fragen der IT-Sicherheit sind Richter zudem nicht weisungsfrei.[33] Richterliche Unabhängigkeit befreit nicht von der Einhaltung von Sicherheitsbestimmungen. Allgemein finden sich vermehrt kritische Stimmen, die unter Sicherheitsgesichtspunkten das Konzept BYOD in Frage stellen. So hat auch das BSI in seinem Überblickspapier Consumerisation und BYOD[34] die Herausforderungen für den Datenschutz betont und sich in der Tendenz sehr zurückhaltend zum allgemeinen Konzept von BYOD geäußert.

5. Zusammenfassung und Ausblick

Jedenfalls lässt sich das Konzept BYOD nur mit einem straff organisierten System von Überwachungs- und Kontrollrechten bis hin zu Möglichkeiten disziplinarischer Maßnahmen[35] verantwortbar umsetzen. Richter sind aber unter dem Aspekt der richterlichen Unabhängigkeit an sich engmaschige Kontrollsysteme – wie regelmäßige Schulungen – bereits im Ansatz nicht gewohnt. Zudem sind die Justizdaten, insbesondere im Bereich des Strafrechts oder Familienrechts, als besonders sensibel (vgl. § 3 Abs. 9 BDSG) und daher als besonders schutzwürdig einzustufen. Strukturell vorhersehbare Sicherheitsdefizite und -risiken können daher in diesem Bereich nicht akzeptiert werden. Im Gegenteil verlangt das Arbeiten mit besonders sensiblen Daten nach häufigeren und umfangreicheren Überprüfungen als das Arbeiten mit normalen Daten.[36] Bei diesen Kontrollmaßnahmen müsste jedoch gewährleistet sein, dass unter inhaltlichen Aspekten – z.B. subtile Einflussnahme auf Sachentscheidungen – der Gedanke der richterlichen Unabhängigkeit unbeschädigt bleibt. Insoweit sind Grundsatzkonflikte vorprogrammiert.

Bei einer Gesamtschau kann daher das Konzept BYOD für die Richter nicht befürwortet werden. Für die weiterhin anzustrebende Möglichkeit einer Heimarbeit müssen andere Konzepte (z.B. Nutzung dienstlicher Geräte) geprüft werden. Eines ist bei der zuvor skizzierten Problematik jedoch deutlich geworden: Erfahrungen, Strategien und Techniken aus der Papierwelt reichen bei der Umstellung auf die digitale Aktenführung allein nicht mehr aus. Dies gilt auch für Fragen der richterlichen Unabhängigkeit.

---

32 Heldmann (Fn. 8), S. 38 ff. m.w.N.

33 So deutlich Berlit (Fn. 16), S. 336.

34 BSI (Fn. 10), S. 8, 9.

35 Vgl. in diesem Zusammenhang auch LAG Rheinland-Pfalz, Urteil vom 12. November 2015, 5 Sa 10/15, MMR 2016, 571: Das private Herunterladen von Software am Arbeitsplatz kann eine außerordentliche Kündigung rechtfertigen, wenn hierdurch ein Computervirus installiert wird und der Arbeitnehmer eine Warnmeldung des Virenscanners missachtet.

36 So Schultze-Melling, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2. Aufl. 2013, § 9 Rn. 14.