Zeitschrift des Bernischen Juristenvereins

Revue de la société des juristes bernois

152. Jahrgang
Erscheint
jeden Monat
Mai
2016

5 2016
www.zbjv.ch

ZBJV

Organ für schweizerische Rechtspflege und Gesetzgebung

Redaktoren
Prof. Dr. Jörg Schmid
Prof. Dr. Sibylle Hofer

Stämpfli Verlag AG Bern



Stämpfli Verlag

Internet am Arbeitsplatz

Ausgewählte arbeitsrechtliche Fragestellungen

Von Isabelle Wildhaber/Silvio Hänsenberger[1]

Inhaltsübersicht

I. Einleitung

II. Internetnutzung mit Konsequenzen

1. Private Nutzung des Internets und unsachgemässe geschäftliche Nutzung des Internets
2. Gefährdung der Interessen des Arbeitgebers
3. Mögliche Sanktionen und Rechtsfolgen

III. Schutz des Arbeitnehmers vor Persönlichkeitsverletzungen

1. Schutz der persönlichen Daten des Arbeitnehmers
2. Schutz vor Cybermobbing
3. Behandlung der über berufliche soziale Netzwerke geknüpften Kontakte bei Anstellungsende
4. Screening von Stellenbewerbern

IV. Bring Your Own Device (BYOD)

1. Kostenteilung
2. Zugang des Arbeitgebers zum BYOD-Gerät
3. Widersprüche zum Arbeitsgesetz (ArG)

V. Elektronische Überwachung der Internetnutzung

1. Grundsätze des DSG und des Art. 26 ArGV 3
2. Aktuelle Rechtsprechung

---

1 Prof. Dr., LL. M., Ordinaria für Privat- und Wirtschaftsrecht unter besonderer Berücksichtigung des Arbeitsrechts an der Universität St. Gallen/M. A. HSG, wissenschaftlicher Assistent.

Ein grosses Dankeschön an Dr. Adrian von Kaenel für die Überlassung des unpublizierten Vortrages «Rechte und Pflichten der Arbeitnehmer im Umgang mit Social Media», ISSS-Tagung Zürich 2011, «Soziale Netzwerke – Informationsquelle oder Risikoherd?», dessen Überlegungen in diesen Aufsatz eingeflossen sind. Herzlichen Dank auch an Dr. Roger Rudolph für den wertvollen Gedankenaustausch.

VI. Nutzungsreglemente

1. Regelungskompetenz des Arbeitgebers
2. Regelung durch Nutzungsreglemente

VII. Schlusswort

I. Einleitung

Knapp die Hälfte (47%) der Schweizer Gesamtbevölkerung nutzte im Jahr 2015 das Internet am Arbeitsplatz.[2] Die zunehmende Digitalisierung der Arbeitswelt verstärkt den Trend zu einer «Entgrenzung» der Arbeit im Sinne der Aufhebung klarer Grenzen zwischen Wohn- und Arbeitsort und zwischen Arbeits- und Freizeit.[3] Die feine Linie zwischen beruflicher und privater Nutzung des Internets verschwimmt zunehmend.[4] Immer häufiger stellen Arbeitgeber ihren Arbeitnehmern ein Smartphone oder Tablet zur Verfügung, welches diese für berufliche, aber auch private Zwecke nutzen können. Auch das umgekehrte «Bring Your Own Device» (BYOD, siehe unten IV.) birgt ähnliche Probleme der Differenzierung zwischen beruflicher und privater Sphäre. Für die Rechtspraxis stellt sich deshalb die grosse Herausforderung, zwischen den berechtigten Interessen der Arbeitnehmer und Arbeitgeber sachgerechte Abwägungen vorzunehmen.

Dieser Beitrag soll einige ausgewählte arbeitsrechtliche Fragen im Zusammenhang mit der Nutzung des Internets bei der Arbeit analysieren (nachfolgend unter II. bis V.) und aufzeigen, wie mit entsprechenden Fragestellungen umgegangen werden sollte, um alle Betei-

2 Bundesamt für Statistik, Internetnutzung in der Schweiz nach Nutzungsort, Entwicklung 1997–2015, abrufbar unter <http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html/>.

3 Wolfgang Däubler, Entgrenzung der Arbeit – Ein Problem des Arbeitsrechts?, Soziales Recht 2014, S. 45 ff.

4 Daniel Alder, E-Mail-Daten am Arbeitsplatz im Fokus von Datenschutz- und Arbeitsrecht, Revue de l'avocat 2013, S. 276 ff., S. 277; Jean-Philippe Dunand, Internet au travail: droits et obligations de l'employeur et du travailleur, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 33 ff., S. 39; Carole Aubert/Régine Delley, Utilisation des réseaux sociaux par les travailleurs et les employeurs, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 133 ff.

ligten zu sensibilisieren, aber auch bestehende Risiken zu minimieren (am besten mittels eines Nutzungsreglements, nachfolgend unter VI.).

II. Internetnutzung mit Konsequenzen

Die private Nutzung des Internets sowie die unsachgemässe geschäftliche Nutzung des Internets können verschiedene arbeitsvertragliche Pflichten und Nebenpflichten des Arbeitnehmers verletzen. Der Arbeitnehmer kann seine Pflicht zur Leistung von Arbeit nach *Art. 319 Abs. 1 OR* oder aber seine Sorgfalts- und Treuepflicht nach *Art. 321a Abs. 1 OR* verletzen. Die Treuepflicht verlangt vom Arbeitnehmer u. a., dass er Schädigungen vermeidet, Weisungen befolgt (Art. 321d Abs. 2 OR) und Geheimhaltung bewahrt (Art. 321a Abs. 4 OR).

1. Private Nutzung des Internets und unsachgemässe geschäftliche Nutzung des Internets

Bei der Nutzung des Internets während der Arbeitszeit ist zwischen der dienstlichen und der privaten Nutzung zu differenzieren. Die dienstliche Nutzung ist Teil der Arbeitsleistung durch den Arbeitnehmer. Für die Unterscheidung kommt es dabei darauf an, ob die Aktivität des Arbeitnehmers *privat oder geschäftlich veranlasst* ist.[5] Wann welcher Fall vorliegt, kann anhand des Zwecks der Nutzung des Internets festgestellt werden. Sobald der Arbeitnehmer die Absicht hatte, die von ihm geforderten Arbeitsleistungen voranzubringen, liegt eine geschäftliche Nutzung vor, unabhängig davon, ob die Nutzung im Einzelfall zweckmässig war.[6] Die Unterscheidung zwischen privater und geschäftlicher Nutzung ist relevant in Bezug auf die Weisungs- und Kontrollmöglichkeiten des Arbeitgebers (siehe unten VI.1.). Die Regelungskompetenz des Arbeitgebers bezüglich privater Nutzung ist nämlich sehr beschränkt.

5 Vgl. Andreas Borsutzky, Soziale Netzwerke, Regelungskompetenz des Arbeitgebers und Mitbestimmungsrechte des Betriebsrats, NZA 2013, S. 647 ff.

6 Dunand (Fn. 4), S. 38; Christoph Holenstein, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Diss. Bern, Bern 2002, S. 71 ff.

Eine exzessive private Nutzung des Internets während der Arbeitszeit kann zu einer Verletzung der Leistungs- und Treuepflicht des Arbeitnehmers infolge *Produktivitätsverlusts* des Unternehmens führen.[7] Es kann zu einer erheblichen Beeinträchtigung der arbeitsvertraglich geschuldeten Leistung kommen, weil der Arbeitnehmer nicht zur Erledigung von privaten Angelegenheiten angestellt wurde. Die private Nutzung des Internets bzw. die unsachgemässe geschäftliche Nutzung können auch deshalb im Widerspruch mit der Treuepflicht des Arbeitnehmers stehen, weil sie zu einer Verletzung der *Reputation* des Unternehmens oder zu einem *Sicherheitsrisiko* für das Unternehmen führen.[8]

2. Gefährdung der Interessen des Arbeitgebers

Eine Verletzung der arbeitsvertraglichen Leistungspflicht nach Art. 319 OR oder der Sorgfalts- und Treuepflicht nach Art. 321a Abs. 1 OR kann durch verschiedenste (von uns teilweise schon anderorts beschriebene[9]) *Handlungen des Arbeitnehmers mit Bezug zum Internet* entstehen. Dabei gilt es zu beachten, dass «Postings» auf Social

7 BGE 139 II 7; BGer 4C./2001 vom 13. 2. 2002, E. 3c; BVGer vom 8./9. 12. 2015, A-5641/2014 und A-6453/2014 (noch nicht rechtskräftig; fristlose Kündigung zweier SBB-Angestellter, die während der Arbeitszeit stundenlang pornografische Websites besucht hatten).

8 So explizit der SBB-Fall, BVGer A-5641/2014 vom 8. 12. 2015, E. 8 und 9; siehe auch Adrian Staehelin, Der Arbeitsvertrag. Art. 319–330a, in: Peter Gauch/Jörg Schmid (Hrsg.), Zürcher Kommentar zum schweizerischen Zivilrecht, Bd. V/2c, 4. Aufl., Zürich 2006, Art. 321 N 23; Jean-Philippe Dunand, L'usage de l'Internet sur le lieu de travail au vu de la jurisprudence récente du Tribunal fédéral, in: Julien Perrin (Hrsg.), Internet au lieu de travail, Lausanne 2004, S. 1 ff., S. 7 f., m. w. H.; Dunand (Fn. 4), S. 33 ff., S. 36 ff., S. 41 f. Vgl. auch Philipp Byers/Stefan Mössner, Die Nutzung des Web 2.0 am Arbeitsplatz: Fluch und Segen für den Arbeitgeber, BB 2012, S. 1665 ff., S. 1666.

9 Isabelle Wildhaber/Silvio Hänsenberger, Kündigung wegen Nutzung von Social Media – wenn Arbeit und Privatleben kollidieren, in: Recht im digitalen Zeitalter, FS Schweizerischer Juristentag 2015, St. Gallen 2015, S. 399 ff. (zit. Recht im digitalen Zeitalter); Kurzfassung: Isabelle Wildhaber/Silvio Hänsenberger, Kündigungsfalle Social Media, sui-generis 2015, S. 77 ff., auf <http://sui-generis.ch/14>, 8. 6. 2015 (zit. sui-generis).

Media i. d. R. als öffentlich einzustufen sind und somit u. E. keinen besonderen Schutz als Kommunikation unter Freunden geniessen,[10] es sei denn, sie fänden tatsächlich nur in einem nicht öffentlichen Rahmen unter einer Handvoll Menschen statt,[11] was selten der Fall sein wird.

Eine *Verletzung der Treuepflicht* kann entstehen, indem der Arbeitnehmer z. B.

- durch ein «Posting» im Internet (schädigende Äusserungen, Veröffentlichen von Fotos oder Videos aus dem Arbeitsumfeld) den Ruf seines Arbeitgebers riskiert;[12]
- seine Geheimhaltungspflicht durch Verrat von Betriebs- und Geschäftsgeheimnissen im Internet verletzt;
- Daten, welche Schadsoftware enthalten oder enthalten könnten, herunterlädt;[13]
- seine Arbeitskollegen cybermobbt;
- die IT-Systemsicherheit des Arbeitgebers gefährdet;
- für einen unautorisierten Auftritt des Arbeitgebers «sorgt»;[14] oder
- den Arbeitgeber der Gefahr einer straf- oder zivilrechtlichen Haftung oder eines anderweitigen rechtlichen Risikos aussetzt.

10 Dazu Jobst-Hubertus Bauer/Jens Günther, Kündigung wegen beleidigender Äusserungen auf Facebook – vertrauliche Kommunikation unter Freunden?, NZA 2013, S. 67 ff., S. 68; vgl. auch Aubert/Delley (Fn. 4), S. 159 f., m. w. H.

11 Wildhaber/Hänsenberger, Recht im digitalen Zeitalter (Fn. 9), S. 408 f.; ebenfalls von einer Handvoll Menschen als Abgrenzungsmerkmal spricht Antje Burmester, Die «Facebook-Kündigung» im Spiegel der aktuellen Rechtsprechung, ArbRB 2013, S. 245 ff.

12 Siehe dazu z. B. den Fall «Inside Paradeplatz», ArbGer ZH vom 11. 12. 2014, AH140052-L, OGer ZH vom 27. 3. 2015, LA150002-O/U. Vgl. auch Jascha Schneider-Marfels, Rufmord im Internet, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, S. 189 ff.

13 Ullin Streiff/Adrian von Kaenel/Roger Rudolph, Arbeitsvertrag. Praxiskommentar zu Art. 319–362 OR, 7. Aufl., Zürich 2012, Art. 328b N 17; Adrian von Kaenel, Internet und Datenschutz am Arbeitsplatz, in: Rolf H. Weber/Reto M. Hilty/Rolf Auf der Maur (Hrsg.), Geschäftsplattform Internet II, Zürich 2001, S. 21 ff., S. 42 f.; Dunand (Fn. 4), S. 43.

14 Vgl. dazu Oliver Staffelbach, Social-Media-Auftritte einrichten, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, S. 1 ff.

Um zu bestimmen, ob eine Verletzung der Leistungs- oder Treuepflicht vorliegt, sind *verschiedene Kriterien* zu berücksichtigen:[15]

1. Beeinträchtigt das Verhalten des Arbeitnehmers die Erfüllung der arbeitsvertraglich vereinbarten *Leistung?*
2. Entstehen dem Arbeitgeber aus der privaten/unsachgemässen Nutzung des Internets durch den Arbeitnehmer bedeutende *finanzielle Kosten,* sei es in Gestalt von Gebühren, Kosten für zusätzlichen Speicherplatz oder von Zeit, die als Arbeitszeit bei der jeweiligen Person verloren geht?[16]
3. Führt die private/unsachgemässe Verwendung des Internets oder von Social Media zu *Sicherheitsrisiken* im Verantwortungsbereich des Arbeitgebers?[17]
4. Gefährdet die Handlung des Arbeitnehmers die *Reputation* des Arbeitgebers in unzulässiger Weise?
5. Verstösst der *Inhalt* der Mitteilungen oder der Nutzung gegen geltendes Recht oder die Sittlichkeit (z. B. der Besuch pornografischer Websites, Cybermobbing)?[18]
6. Steht der Internetnutzung ein *ausdrückliches Verbot* des Arbeitgebers entgegen?

3. Mögliche Sanktionen und Rechtsfolgen

Ergeben diese Kriterien, dass eine Verletzung der arbeitsvertraglichen Leistungspflicht nach Art. 319 OR oder der Treuepflicht nach Art. 321a Abs. 1 OR vorliegt, so kann dies verschiedene Sanktionen und Rechtsfolgen für den Arbeitnehmer mit sich bringen.

15 So schon WILDHABER/HÄNSENBERGER, Recht im digitalen Zeitalter (Fn. 9), S. 402 f.; ähnlich DUNAND (Fn. 4), S. 41 ff.; AUBERT/DELLEY (Fn. 4), S. 141.

16 Vgl. DUNAND (Fn. 4), S. 42 f., HOLENSTEIN (Fn. 6), S. 37 f., S. 83; STREIFF/VON KAENEL/RUDOLPH (Fn. 13), Art. 328b N 17.

17 Vgl. DUNAND (Fn. 4), S. 43; HOLENSTEIN (Fn. 6), S. 83.

18 BGer 4C.109/2003 vom 30.7.2003, E. 2.2.1; BGer 4C.349/2002 vom 25.6.2003, E. 5. Vgl. dazu auch FLORIAN SCHMIDT-GABAIN, Social Media und Inhalte, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, S. 43 ff.

a. *Kündigung*

Die Internetnutzung des Arbeitnehmers kann, wie an anderer Stelle von uns schon ausführlich analysiert,[19] zu dessen *ordentlicher oder fristloser Kündigung* führen.

Aus der vertraglichen Treuepflicht des Arbeitnehmers kann nicht gefolgert werden, dass es dem Arbeitnehmer grundsätzlich verwehrt ist, sich kritisch über seine Arbeit, sein Arbeitsverhältnis, den Arbeitgeber oder dessen Kunden und Geschäftspartner zu äussern,[20] u. U. auch überspitzt. Bei der insoweit notwendigen Abwägung zwischen Meinungsäusserungsfreiheit und Treuepflicht kommt es massgeblich auf den Inhalt und die Einzelumstände des «Postings» an (wie die Schwere der Beeinträchtigung des Unternehmens, den sprachlichen Kontext, den zu verantwortenden Verbreitungsgrad, den Schutz der persönlichen Verhältnisse und der Ehre anderer Personen usw.). Ist die Kritik durch den Arbeitnehmer sachlich, objektiv und unpolemisch, so ist sie zulässig und durch die Meinungsäusserungsfreiheit geschützt. Eine ordentliche Kündigung wäre dann *missbräuchlich* gemäss Art. 336 Abs. 1 Bst. b OR. Die Kündigung ist aber *nicht* missbräuchlich, wenn die Meinungsäusserung eine Pflicht aus dem Arbeitsverhältnis verletzt oder die Zusammenarbeit im Betrieb wesentlich beeinträchtigt (Art. 336 Abs. 1 Bst. b OR). Grobe Beleidigungen des Arbeitgebers, der Arbeitskollegen oder der Kunden oder Geschäftspartner des Arbeitgebers, die nach Inhalt und Form zu einer erheblichen Ehrverletzung des Betroffenen führen, können deshalb eine ordentliche und nicht missbräuchliche Kündigung nach sich ziehen.[21]

19 WILDHABER/HÄNSENBERGER, Recht im digitalen Zeitalter (Fn. 9), S. 401 ff.

20 CHRISTIANE BRUNNER/JEAN-MICHEL BÜHLER/JEAN-BERNARD WAEBER/CHRISTIAN BRUCHEZ, Kommentar zum Arbeitsvertragsrecht, 3. Aufl., Basel 2005, N 5; MARTIN FARNER, Missbräuchliche Kündigung (Art. 336 Abs. 1 Bst. a OR), Kritik am Vorgesetzten, Bemerkungen zum Urteil des Bundesgerichts, I. Zivilabteilung, 19. 12. 2000, M. c. R., Berufung, AJP 2001, S. 710 ff.; MARTIN KOCK, Unmutsäusserungen und Beleidigungen auf Facebook & Co. als Kündigungsgrund, DB 2013, S. 934 ff. Vgl. auch Trib. NE vom 10. 2. 2012, Cour de droit public, No. CDP.2010.45.

21 Fall «Inside Paradeplatz» (Fn. 12), schwere Treuepflichtverletzung durch den Kommentar «Da der oberste Chef kein Rückgrat hat, fehlen auch den Chefs auf den tiefsten Stufen die Eier» auf dem öffentlich zugänglichen Onlineportal «Inside Paradeplatz».

Eine *fristlose Kündigung* dürfte indessen nur bei mutwilligen und besonders schwerwiegenden Verstössen angezeigt sein. Um im entsprechenden Einzelfall feststellen zu können, ob ein wichtiger Grund gegeben ist, kann mitberücksichtigt werden, ob der Arbeitgeber klare Anordnungen zur Benutzung der elektronischen Kommunikationsmittel erlassen hat, ob er sich früher bereits eindeutig gegen die missbräuchliche Nutzung des Internetzuganges oder sogar diesbezügliche Verweise oder Verwarnungen[22] ausgesprochen hat. Darüber hinaus können ferner die Stellung und Verantwortung des betroffenen Arbeitnehmers im Betrieb, die Art des Betriebs (z. B. Tendenzbetrieb, Kleinbetrieb, Tätigkeitsbereich eines Unternehmens usw.), die Intensität des Vertrauensverhältnisses sowie die Existenz und die Schwere des Verschuldens des Arbeitnehmers miteinbezogen werden.[23]

b. *Schadenersatzforderung des Arbeitgebers*

Basierend auf der Verletzung der Treuepflicht gemäss Art. 321a Abs. 1 OR infolge privater oder geschäftlicher Nutzung des Internets kann eine *Schadenersatzforderung des Arbeitgebers gegenüber dem Arbeitnehmer* entstehen (Art. 321e OR[24]), welche in den Schranken von Art. 323b Abs. 1 OR mit dem Lohn verrechenbar ist.[25] Für die Feststellung der Treuepflicht kann es entscheidend sein, ob der Arbeitgeber den Arbeitnehmer vorgängig über seine Pflichten im Rahmen der Internetnutzung informiert hat. Relevant dafür ist der individuelle Arbeitsvertrag inkl. Nutzungsreglement.[26]

c. *Lohnausfall*

Erfolgt eine private Internetnutzung in einem solchen Ausmass, dass von einer Arbeitsleistung im Interesse des Arbeitgebers nicht mehr die Rede sein kann, so schuldet der Arbeitgeber dem Arbeitneh-

22 BGer 4A.430/2008 vom 24. 11. 2008, E. 4 (kurze Nutzung des Internets hat trotz Verwarnung nicht für eine fristlose Kündigung ausgereicht).

23 BGE 127 III 310 E. 3.

24 Siehe zur Praxis ausführlich Stefanie Meier-Gubser, Haftung des Arbeitnehmers, TREX 2012, S. 292 ff.

25 Staehelin (Fn. 8), Art. 322 N 5; Holenstein (Fn. 6), S. 157 f.; Dunand (Fn. 4), S. 45 f.

26 Mark A. Reutter/Samuel Klaus, Rechtliche Stolpersteine bei «BYOD», digma 2012, S. 160 ff., S. 165.

mer für den fraglichen Zeitraum keinen Lohn.[27] Ein derartiger *Ausfall des Lohnanspruches* wird selten nachgewiesen werden können.

d. *Strafrechtliche Konsequenzen*

Die widerrechtliche Nutzung eines Internetzugangs durch den Arbeitnehmer kann zu *strafrechtlichen Konsequenzen* führen. Die Benutzung des Internetzugangs hinterlässt, sofern keine aufwendigen technischen Gegenmassnahmen getroffen werden, eine Datenspur im Internet, welche anhand der IP-Adresse dem Arbeitgeber zugeordnet werden kann. Dadurch können Arbeitgeber bzw. Arbeitnehmer in den Fokus der Strafverfolgungsbehörden geraten, falls der Internetzugang für widerrechtliche Aktivitäten verwendet wurde.[28] Zu denken ist insbesondere an üble Nachrede (Art. 173 StGB), Verleumdung (Art. 174 StGB), Beschimpfung (Art. 177 StGB)[29], den Konsum oder das Zugänglichmachen von qualifiziertem pornografischem Material (Art. 197 Abs. 4 und 5 StGB), Rassendiskriminierung (Art. 261bis StGB), das Verbreiten anderweitig illegaler Inhalte, unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB) oder die unbefugte Datenbeschaffung (Art. 143 StGB). Ebenfalls in Betracht fallen Normen des Nebenstrafrechts wie zum Beispiel Urheberrechtsdelikte (Art. 71 URG) oder Wettbewerbsdelikte (Art. 26 UWG).

e. *Zivilrechtliche Haftung gegenüber Dritten*

Bei einer widerrechtlichen Nutzung des Internetzugangs besteht das Risiko einer zivilrechtlichen Haftung des Arbeitgebers oder des Arbeitnehmers gegenüber Dritten. Handelt es sich beim Geschädigten um einen Vertragspartner des Unternehmens (z. B. Kunden oder Lieferanten), ist zunächst die *vertragliche Haftung* für Hilfspersonen nach Art. 97 i. V. m. Art. 101 OR zu prüfen.[30] Besteht kein Vertrag mit dem

27 Holenstein (Fn. 6), S. 157; Dunand (Fn. 4), S. 41; Michèle Stutz/Noemi Valloni, Social Media im Arbeitsrecht, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, S. 159 ff., S. 171.

28 Holenstein (Fn. 6), S. 43 ff.; Streiff/von Kaenel/Rudolph (Fn. 13), Art. 328b N 17; Dunand (Fn. 4), S. 11 f.

29 BezGer ZH vom 30. 9. 2011, GG110138-L/DU.

30 Wolfgang Wiegand, Basler Kommentar, Obligationenrecht I, Art. 1–529, Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wieland (Hrsg.), 6. Aufl., Basel 2015, Art. 101 N 7 ff.

Geschädigten, kann der Arbeitgeber basierend auf der *Geschäftsherrenhaftung nach Art. 55 Abs. 1 OR* zum Ersatz des Schadens verpflichtet sein. Allerdings kann er sich mit dem Beweis von der Haftung befreien, dass er die notwendige Sorgfalt angewendet hat, um den betreffenden Schaden zu vermeiden,[31] oder dass der Schaden auch bei Anwendung dieser Sorgfalt eingetreten wäre.[32] Dem Sorgfaltsbeweis zuträglich können insbesondere dokumentierte Bemühungen zur Sicherstellung der IT-Sicherheit sowie verbindliche Vorgaben an den Arbeitnehmer zur Internetnutzung sein.[33] Schädigt der Arbeitnehmer den Dritten nur «bei Gelegenheit» der geschäftlichen Verrichtung, ist zu berücksichtigen, inwieweit der Arbeitgeber beispielsweise mittels entsprechender Überwachung oder Selektion dem Risiko der vorsätzlichen Schädigung durch den Arbeitnehmer hätte vorbeugen können.[34]

Dem geschädigten Dritten steht zudem die Möglichkeit offen, seine Ansprüche aufgrund von *Art. 41 OR dem Arbeitnehmer gegenüber direkt* geltend zu machen. In diesem Fall mangelt es dem Arbeitnehmer an der Möglichkeit, sich auf den ermässigten Haftungsmassstab von Art. 321e Abs. 2 OR zu berufen (ansonsten würde das Betriebsrisiko auf den geschädigten Dritten übertragen). Der Arbeitnehmer hat deshalb Anspruch darauf, dass ihn der Arbeitgeber von den direkten Ansprüchen Dritter freihält, falls er den Schaden in Erfüllung seiner Arbeits- oder Treuepflicht verursacht und für ihn nicht selbst aufzukommen hat.[35]

f. *Weitere Sanktionen*

Des Weiteren kann der Arbeitgeber *technische Sperrungen* vornehmen, indem er z. B. gewisse Websites oder Social-Media-Plattformen ganz sperrt oder den Download bestimmter Dateien verun-

31 Roland Brehm, Berner Kommentar, Die Entstehung durch unerlaubte Handlungen, Art. 41–61 OR, Heinz Hausheer/Hans Peter Walter (Hrsg.), 4. Aufl., Bern 2013, Art. 55 N 45 ff.

32 BK-Brehm (Fn. 31), Art. 55 N 91 ff.

33 Reutter/Klaus (Fn. 26), S. 164.

34 BK-Brehm (Fn. 31), Art. 55 N 27 f., m. w. H.; BSK OR I-Wiegand (Fn. 30), Art. 101 N 10, m. w. H.

35 Manfred Rehbinder/Jean-Fritz Stöckli, Berner Kommentar, Einleitung und Kommentar zu den Art. 319–362 OR, Bern 2010, Art. 321e N 27; Streiff/von Kaenel/Rudolph (Fn. 13), Art. 321e N 5.

möglicht.[36] Er kann auch die *im einschlägigen Nutzungsreglement vorgesehenen Sanktionen* verhängen (siehe beides unten VI.2.).

III. Schutz des Arbeitnehmers vor Persönlichkeitsverletzungen

1. Schutz der persönlichen Daten des Arbeitnehmers

Die Bearbeitung personenbezogener Arbeitnehmerdaten durch den Arbeitgeber ist gemäss Art. 328b OR nur zulässig, soweit sie die Eignung des Arbeitnehmers für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.[37] Diese Bestimmung bezweckt den Schutz der Persönlichkeit des Arbeitnehmers über das DSG hinaus und hat selbständige Bedeutung.[38] Dabei ist Art. 328b OR nicht als Verbotsnorm aufzufassen, deren Verletzung eine unerlaubte Handlung darstellt. Vielmehr handelt es sich sowohl um relativ zwingendes Arbeitsvertragsrecht als auch um einen auf Arbeitsverhältnisse beschränkten Bearbeitungsgrundsatz.[39] Art. 328b OR ist Ausfluss der Fürsorgepflicht des Arbeitgebers im Sinne von Art. 328 OR.

Aufgrund der Eigenschaft von Art. 328b OR als Arbeitsvertragsrecht stellt dessen Missachtung durch den Arbeitgeber eine Vertragsverletzung dar.[40] Als Bearbeitungsgrundsatz ergänzt die Regelung von Art. 328b OR die nicht abschliessende Aufzählung von Art. 12 Abs. 2 Bst. a DSG. Letztere Bestimmung verweist für die rechtmässige Bearbeitung von Daten zudem auf die Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG. Diese beinhalten unter anderem das

36 Holenstein (Fn. 6), S. 107 ff.

37 Beispiele zur zulässigen und unzulässigen Datenerhebung durch den Arbeitgeber vgl. von Kaenel (Fn. 13), S. 29 ff.

38 Von Kaenel (Fn. 13), S. 23.

39 David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008, Art. 328b N 5.

40 Rosenthal/Jöhri (Fn. 39), Art. 328b N 9. Eine Verletzung des Datenschutzes bei der Bearbeitung von Arbeitnehmerdaten gilt immer auch als Verstoss gegen die Fürsorgepflicht (Art. 328 OR), vgl. dazu Wolfgang Portmann/Roger Rudolph, Basler Kommentar, Obligationenrecht I, Art. 1–529, Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wieland (Hrsg.), 6. Aufl., Basel 2015, Art. 328b N 30.

Zweckbindungsgebot (Art. 4 Abs. 3 DSG), das Erkennbarkeitsgebot (Art. 4 Abs. 4 DSG) sowie die Vorgabe, dass Personendaten durch angemessene technische und organisatorische Massnahmen geschützt werden müssen (Art. 7 Abs. 1 DSG). Eine Missachtung eines Bearbeitungsgrundsatzes hätte somit neben vertraglichen Ersatzansprüchen auch deliktische Ansprüche des Arbeitnehmers aus Persönlichkeitsverletzung zur Folge.[41]

Für die Verletzung des Bearbeitungsgrundsatzes von Art. 328b OR gibt es gestützt auf Art. 13 Abs. 1 DSG verschiedene Rechtfertigungsgründe. Im Rahmen des Arbeitsverhältnisses sind folgende Rechtfertigungsgründe möglich:[42]

- *Gesetzesbestimmung.* Beispiel: Der Arbeitgeber bewahrt ein geschäftliches E-Mail des Arbeitnehmers auf, welches auch Informationen ohne Arbeitsplatzbezug enthält. Dies kann gemäss Art. 957 OR (Pflicht zur Buchführung und Rechnungslegung) gerechtfertigt sein.
- *Überwiegendes privates oder öffentliches Interesse.* Beispiel: Der Arbeitgeber sichert ein privates E-Mail des Arbeitnehmers auf seinem Server, weil er dieses nur mit unverhältnismässig hohem Aufwand von den geschäftlichen Daten trennen kann.
- *Einwilligung.* Beispiel: Der Arbeitgeber speichert auch Daten über den Verlauf der privaten Internetnutzung, nachdem der Arbeitnehmer Internet-Guidelines unterschrieben hat, in welchen er seine ausdrückliche Zustimmung zu diesem Vorgehen gegeben hat.

Schliesslich hat der Arbeitgeber gemäss Art. 14 Abs. 1 DSG eine Informationspflicht, falls er besonders schützenswerte Personendaten (im Sinne von Art. 3 Bst. c DSG) über seine Arbeitnehmer sammelt oder Persönlichkeitsprofile (im Sinne von Art. 3 Bst. d DSG) anfertigt.

41 BSK OR I-Portmann/Rudolph (Fn. 40), Art. 328b N 10.

42 Vgl. Rosenthal/Jöhri (Fn. 39), Art. 328b N 12 f.; David Vasella, Social Media und Datenschutz, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, S. 251 ff., S. 266 ff.; von Kaenel (Fn. 13), S. 27.

2. Schutz vor Cybermobbing

Internet am Arbeitsplatz eröffnet das Risiko für Cybermobbing. *Cybermobbing* ist das systematische Anfeinden, Schikanieren oder Diskriminieren unter Arbeitnehmern oder durch Vorgesetze mithilfe elektronischer Kommunikationsmittel bzw. neuer Kommunikationsmedien.[43] Cybermobbing verletzt sowohl Art. 28 ff. ZGB und Art. 328 OR als auch Art. 6 ArG und Art. 2 ArGV 3. Cybermobbing ist zu unterscheiden von einer *virtuellen sexuellen Belästigung* des Arbeitnehmers (z. B. durch E-Mails mit pornografischem Inhalt oder durch «Posten» von sexistischen Bemerkungen).[44] Die sexuelle Belästigung am Arbeitsplatz (Art. 198 StGB) verletzt nicht nur Art. 328 OR, sondern stellt auch eine Diskriminierung im Sinne von Art. 4 Satz 1 GlG dar.[45]

Hinsichtlich der Handlungspflichten und -möglichkeiten des Arbeitgebers in Bezug auf Ausgrenzungen in der virtuellen Welt bestehen *grosse Unsicherheiten.*[46] Für den Arbeitgeber ist es wichtig, den Umfang seiner Fürsorgepflichten zu kennen, um Haftungsrisiken vorzubeugen. Handlungspflichten des Arbeitgebers bestehen nur dann, wenn das Cybermobbing *für das Beschäftigungsverhältnis relevant*

43 Zum Begriff BSK OR I-Portmann/Rudolph (Fn. 40), Art. 328 N 19 ff.; Jean-Philippe Dunand, Le harcèlement psychologique (mobbing) en droit privé suisse du travail, RJN 2006, S. 13 ff.; Eidg. PRK vom 10. 5. 2001, PRK 2000-056 (Cybermobbing); BezGer ZH GG110138-L/DU vom 30. 9. 2011 (Cybermobbing); BGer 8C.446/2010 vom 25. 1. 2011, E. 4.1 (Mobbing); BGer 4A.245/2009 vom 6. 4. 2010, E. 4.2 (Mobbing).

44 Zum Begriff Art. 4 Satz 1 GlG sowie BSK OR I-Portmann/Rudolph (Fn. 40), Art. 328 N 40. Vgl. auch BGE 126 III 395 E. 7b/bb; BGer 4C.289/2006 vom 5. 2. 2007, E. 3.1; BGer 4A.178/2010 vom 14. 5. 2010.

45 Ein Opfer kann Entschädigungsansprüche gemäss Art. 5 Abs. 3 GlG geltend machen, sollte der Arbeitgeber nach Bekanntwerden eines Vorfalles keine zumutbaren Schutzmassnahmen ergreifen. Der Arbeitgeber kann die ausbezahlte Entschädigung anschliessend beim schädigenden Arbeitnehmer zurückfordern, siehe Streiff/von Kaenel/Rudolph (Fn. 13), Art. 328 N 5; Jean-Philippe Dunand/Sandrine Tornare, L'obligation de l'employeur de prévenir les conflits interpersonnels (sources, concrétisation et responsabilité), in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Conflits au travail – Prévention, gestion, sanctions, Genève/Zurich/Bâle 2015, S. 36 ff.

46 Dunand/Tornare (Fn. 45), S. 29 ff.; Vincent Carron, Mobbing et demeure de l'employeur, in: Rémy Wyler (Hrsg.), Panorama en droit du travail, Bern 2009, S. 115 ff. Vgl. auch Thomas Hey, Cybermobbing – Welche Pflichten treffen den Arbeitgeber?, BB 2013, S. 2805 ff.

ist, was auch dann der Fall sein kann, wenn das Mobbing im Internet stattfindet. Zwar rechtfertigt das rein private Verhalten des Arbeitnehmers i. d. R. noch keine arbeitsrechtlichen Massnahmen des Arbeitgebers. Bei Cybermobbing gilt es aber zu bedenken, dass «Postings» meistens keinen Schutz als private Kommunikation unter Freunden geniessen («Postings» gelten meistens als «öffentlich», siehe oben II. 2.) und dass sie konkret das Arbeitsverhältnis berührende Auswirkungen haben können. Beleidigende Äusserungen über Arbeitskollegen verlieren ihren betrieblichen Charakter nicht schon dadurch, dass sie über soziale Netzwerke oder ausserhalb der Arbeitszeiten erfolgen. Dies muss umso mehr gelten, wenn es sich um berufsbezogene Netzwerke wie Xing oder LinkedIn oder gar die eigene Firmenwebsite handelt, da hier bewusst eine Beziehung zum Arbeitgeber hergestellt wird.

Ausserdem kann man womöglich in Fällen von Cybermobbing schneller das Vorliegen der für Mobbing erforderlichen Systematik annehmen, wenn man die höhere Intensität, die längere Lebensdauer und den Effekt der Multiplikation im Internet berücksichtigt.[47] Die Betroffenen werden das Gefühl des Kontrollverlustes oft stärker erleben als beim klassischen Mobbing: Im Internet kann eine einmalige Beleidigung die gleichen Auswirkungen haben wie mehrmalige Mobbingangriffe im Alltag. Die einmalige Opferrolle setzt sich beliebig fort, da man nicht weiss, wie viele Menschen die Beleidigungen schon gesehen haben oder ob sie irgendwo wieder auftauchen, wenn sie an der einen Stelle gelöscht wurden.[48]

Die *Fürsorgepflicht des Arbeitgebers* (Art. 328 OR) verlangt, dass dieser die physische und psychische Integrität des Arbeitnehmers schützt, was auch die Achtung seiner Persönlichkeit impliziert. Bei Cybermobbing ist der Arbeitgeber zum Einschreiten verpflichtet, es bestehen also Handlungspflichten, wenn die Persönlichkeit eines Arbeitnehmers durch Vorgesetzte oder Mitarbeiter verletzt oder gefährdet ist.[49] Aus Art. 328 OR kann eine *Pflicht zu präventiven Massnah-*

47 Zum Effekt der Multiplikation siehe WILDHABER/HÄNSENBERGER, Recht im digitalen Zeitalter (Fn. 9), S. 418 f.

48 DANIEL SÜSS, in: Suva, Früherkennungsradar, Luzern 2012, S. 63.

49 ANTONIA ULRICH, Mobbing am Arbeitsplatz, Sicherheit & Recht, 2014, S. 223 ff., S. 225; SECO, Mobbing und andere Belästigungen, Schutz der persönlichen Integrität am Arbeitsplatz, Bern 2013, S. 29 ff.

men bei Cybermobbing abgeleitet werden.[50] Der Arbeitgeber hat seinen Mitarbeitern demnach u. U. die Problematik und die Konsequenzen von Mobbing und Cybermobbing aufzuzeigen.[51] Die Pflicht zu präventiven Massnahmen umfasst ferner den Zugang zu einer unabhängigen Vertrauensperson wie auch Schlichtung, Beratung und Unterstützung.[52] Verschiedene Unternehmen wie Novartis, Swisscom oder UBS verfügen über Betriebsvereinbarungen, welche einen Verhaltenskodex sowie Schlichtungs- und Hilfsangebote und Hinweise auf rechtliche Konsequenzen enthalten.[53] Eine Sensibilisierung der Arbeitnehmer ist deshalb so wichtig, weil entsprechende Posts (z. B. auf Social-Media-Plattformen oder in WhatsApp-Nachrichten) durch die rasche Verbreitungsmöglichkeit sehr schnell eine persönlichkeitsverletzende Schwere erreichen[54] und nicht zuletzt das Betriebsklima erheblich beeinträchtigen können.

Liegen sodann konkrete Verdachtsmomente des Cybermobbings vor, muss der Arbeitgeber den Sachverhalt aufklären. Eine *Pflicht zur Aufklärung* besteht dann, wenn der Arbeitgeber von den entsprechenden Anhaltspunkten Kenntnis erlangt oder fahrlässig nicht erlangt

50 Ebenso Sabine Steiger-Sackmann, Schutz vor psychischen Gesundheitsrisiken am Arbeitsplatz. Rechtliche Möglichkeiten zur Verbesserung der Prävention, Diss. Zürich 2012, S. 159 ff.; Jürg Oskar Luginbühl, Schikanen am Arbeitsplatz – rechtliche, gesundheitliche und soziale Aspekte, ARV 2010, S. 65 ff., S. 69; Dunand/Tornare (Fn. 45), S. 32, S. 44 ff.; Carole Sonnenberg, La protection de la personnalité du travailleur: sauvegarde de sa santé et sécurité au travail, Lausanne 2010, S. 67. Vgl. auch BGE 132 III 257, E. 5.4.4.

51 Vgl. Burkhard Göpfert/Carolin Siegrist, Stalking – Nach Inkrafttreten des Allgemeinen Gleichbehandlungsgesetzes auch ein Problem für Arbeitgeber?, NZA 2007, S. 473 ff., S. 476.

52 Siehe ausführlich Dunand/Tornare (Fn. 45), S. 52 ff.; SECO, Mobbing (Fn. 49), S. 30. Vgl. auch BGer 2C.462/2011 vom 9.5.2012, E. 4.3 (die kantonale Behörde könne gestützt auf Art. 6 ArG «la désignation d'une personne de confiance dans le but de prévenir les conflits internes pouvant survenir en son sein» verlangen); dazu Jean-Philippe Dunand/Sandrine Tornare, «Personne de confiance» et prévention des conflits au travail, in: FS Stöckli, Zürich/St. Gallen 2014, S. 151 ff.

53 Elsbeth Tobler, Mobbing, Den Weg aus der Falle suchen, NZZ vom 10.2.2016, http://www.nzz.ch/wirtschaft/unternehmen/mensch-und-arbeit-in-der-mobbingfalle-ld.5168.

54 Wildhaber/Hänsenberger, Recht im digitalen Zeitalter (Fn. 9), S. 418 f. A. M. Ulrich (Fn. 49), S. 225.

hat. Hierzu hat er «Täter» und «Opfer» anzuhören.[55] Gegebenenfalls hat er das «Opfer» aufzufordern, ihm die entsprechenden Mitteilungen oder «Postings» am Bildschirm oder als Ausdruck zu zeigen. Eine darüber hinausgehende Recherchepflicht des Arbeitgebers ist jedoch ebenso abzulehnen wie die Verpflichtung des Arbeitgebers, dem entsprechenden Netzwerk beizutreten.[56] Ist ein Mobbing-Sachverhalt festgestellt, hat der Arbeitgeber die im Einzelfall *erforderlichen arbeitsrechtlichen Massnahmen zur Unterbindung der Benachteiligung* wie Verwarnung, Umsetzung, Versetzung oder Kündigung zu ergreifen.[57] Insbesondere hat er den fehlbaren Arbeitnehmer aufzufordern, den Eintrag zu löschen und eine (dokumentierte) Unterlassungserklärung abzugeben. Auch wird der Arbeitgeber darauf hinwirken, dass Wiederholungen unterbleiben. Dies kann er tun, indem er z. B. dem «Täter» die Nutzung des sozialen Netzwerkes während der Arbeitszeit untersagt oder indem er Massnahmen für den Fall der Zuwiderhandlung vorsieht, sodass der «Täter» bei Verstoss mit Sanktionen zu rechnen hat und hinreichend gewarnt ist. Eine darüber hinausgehende Überwachungspflicht des Arbeitgebers besteht jedoch nicht. Verletzt der Arbeitgeber seine Schutzpflichten, besteht die Gefahr, dass er dem betroffenen Arbeitnehmer vertraglichen und u. U. ausservertraglichen *Schadenersatz* und/oder *Genugtuung* leisten muss.[58]

3. Behandlung der über berufliche soziale Netzwerke geknüpften Kontakte bei Anstellungsende

Soziale Netzwerke, die den Aufbau und die Pflege beruflicher Kontakte ermöglichen, werden immer beliebter und wichtiger. Die Bewerbung von Produkten, Dienstleistungen und Veranstaltungen findet zunehmend auch über diese sozialen Netzwerke statt. Aufgrund seines Weisungsrechts kann der Arbeitgeber den Arbeitnehmer zu Werbe- und Marketingzwecken anweisen, zwecks Aufbaus von Ge-

55 Vgl. Burkard Göpfert/Carolin Siegrist, Diskriminierungsverdacht: Über den richtigen Umgang mit arbeitsrechtlichen Diskriminierungsfällen, ZIP 2006, S. 1710 ff., S. 1712.

56 So auch Hey (Fn. 46), S. 2805 ff.

57 Zu Massnahmen bei Bekanntwerden von Mobbingvorwürfen siehe BGer 8C.900/2013 vom 5. 5. 2014; Dunand/Tornare (Fn. 45), S. 47 ff.

58 Siehe dazu ausführlich Dunand/Tornare (Fn. 45), S. 59 ff.

schäftsbeziehungen und zur Pflege von Kundenkontakten im Internet, z. B. auf Social-Media-Plattformen, einen Account zu betreiben.[59] Dabei stellt sich bei Beendigung des Arbeitsverhältnisses die Frage, ob er den Social-Media-Account mit dem Netzwerk dem Arbeitgeber überlassen bzw. insbesondere Kundenkontakte im auf den eigenen Namen lautenden beruflichen Netzwerk löschen muss.[60] Diese Frage wurde bis anhin gerichtlich nicht geklärt. Grundsätzlich gilt, dass der Arbeitgeber am Arbeitsergebnis berechtigt ist, das vom Arbeitnehmer in Ausübung seiner vertraglichen Tätigkeit hervorgebracht wird (Art. 321b OR, Art. 339a OR).[61] Knüpft der Arbeitnehmer im Rahmen seiner beruflichen Tätigkeit im Auftrag seines Arbeitgebers geschäftliche Kontakte, hat der Arbeitnehmer dem Arbeitgeber die betreffenden Kontaktinformationen während des Arbeitsverhältnisses (auf Verlangen) jederzeit herauszugeben (Art. 321b OR). Bei Beendigung des Anstellungsverhältnisses sind geschäftliche Kontaktdaten dem Arbeitgeber im Rahmen der Rückgabepflicht zu übergeben (Art. 339a OR).[62]

Eindeutig ist die Rechtslage, wenn der Arbeitnehmer *auf Verlangen und auf Kosten des Arbeitgebers ein Profil angelegt* hat. In der Regel wird dieser Account dem Corporate Design des Unternehmens entsprechen, er wird während der Arbeitszeit genutzt werden und ausschliesslich unternehmensbezogene Kontaktdaten enthalten. In diesem Fall handelt es sich um ein Arbeitsergebnis des Arbeitsgebers, das bei Beendigung des Arbeitsverhältnisses mit Zugangsdaten samt Inhalt herauszugeben ist.

---

59 Stutz/Valloni (Fn. 27), S. 166. So auch in EGMR, Kammerurteil vom 12. 1. 2016, Bărbulescu/Romania, Nr. 61496/08. Weiterführend auch Wildhaber/Hänsenberger, Recht im digitalen Zeitalter (Fn. 9), S. 426 f.

60 Michèle Stutz/Alexandra Geiger-Steiner, Arbeitsrechtliche Fragen rund um Social Media, Anwaltsrevue 2013, S. 212 ff., S. 215 f.; Byers/Mössner (Fn. 8), S. 1670 f.; Roman Frik/Ralf Klühe, Nutzung von Kontakten aus Sozialen Netzwerken während und bei Beendigung des Arbeitsverhältnisses, DB 2013, S. 1174 ff.

61 Zu den urheberrechtlichen Aspekten siehe Vincent Salvadé/Nathalie Tissot, La réalisation d'un site web ou l'ouverture d'un compte par le travailleur. Qui est titulaire des droits?, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 227 ff., S. 243 ff.

62 Vgl. ausführlich Frik/Klühe (Fn. 60), S. 1176; Christian Oberwetter, Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, NJW 2011, S. 417 ff., S. 420; Byers/Mössner (Fn. 8), S. 1670 f.

Schwieriger sieht es aus, wenn der Arbeitnehmer *auf Weisung des Arbeitgebers während des Arbeitsverhältnisses einen Account im eigenen Namen* errichtet und dort in seinem Namen (wenn auch als Mitarbeiter des Arbeitgebers) Kundenkontakte zu pflegen hatte (z. B. auf LinkedIn) oder wenn der Arbeitnehmer seine berufliche Kommunikation über einen ursprünglich für private Zwecke eingerichteten und auch parallel privat genutzten Account abwickelt.[63] Kontakte, welche keinen Bezug zum Arbeitsverhältnis aufweisen, muss der Arbeitnehmer bei Beendigung des Arbeitsverhältnisses nicht an den Arbeitgeber weiterleiten. Solche Kontakte sind nicht «in Ausübung der vertraglichen Tätigkeit» im Sinne von Art. 321b Abs. 2 OR entstanden. Eine Übergabe solcher Daten würde gegen Art. 328b OR verstossen. Zusätzlich könnte eine Weitergabe der Kontaktdaten eine unzulässige Datenbearbeitung darstellen (Art. 12 Abs. 2 Bst. a DSG) und damit die Persönlichkeitsrechte der betroffenen Drittperson unzulässig verletzen – sofern keine Rechtfertigungsgründe (Art. 13 DSG) vorliegen.

Problematisch gestaltetet sich die Situation bei Kontakten, welche nur *bei Gelegenheit der vertraglichen Tätigkeit gewonnen* (z. B. wenn der Arbeitgeber Sponsor einer Sportveranstaltung ist und seine Mitarbeiter als Zuschauer an der Veranstaltung teilnehmen) und/oder *nicht aufgrund der Funktion als Mitarbeiter des Arbeitgebers geknüpft* wurden. Ein Herausgabeanspruch des Arbeitgebers ist in diesem Fall zu bejahen, sofern ein genügender Bezug des Kontaktes zum Arbeitsverhältnis besteht. Parallel dazu ist die datenschutzrechtliche Zulässigkeit der Datenübergabe zu prüfen. War der geschäftliche Hintergrund der Kommunikation mit dem Arbeitnehmer für den Dritten nicht klar ersichtlich, muss der Dritte einer Datenübergabe zustimmen (Art. 4 Abs. 3, Art. 12 Abs. 1 und Art. 13 Abs. 1 DSG). Liegt keine Zustimmung des Dritten vor bzw. würde der Arbeitnehmer mit der Herausgabe die Persönlichkeit des Dritten verletzen, muss der Arbeitgeber auf die Aushändigung der Daten verzichten. In diesem Fall geht seine Fürsorgepflicht (Art. 328 OR) seinem Herausgabe- (Art. 321d) bzw. Rückgabeanspruch (Art. 339a OR) vor.

Elektronische Kontaktinformationen sind teilbar und können trotz Herausgabe beim Arbeitnehmer weiter bestehen. Deshalb stellt

63 Allerdings darf der Arbeitnehmer aufgrund seines Persönlichkeitsrechts nicht dazu angewiesen werden, seinen ursprünglich privat betriebenen Social-Media-Account für geschäftliche Zwecke zu verwenden, wenn er dies nicht will.

sich die Frage, *ob der Arbeitnehmer geschäftliche Kontaktdaten in seinem eigenen Social-Media-Profil löschen muss,* sofern dies der Arbeitgeber verlangt. Aus Art. 339a OR kann nur schwerlich ein Löschungsanspruch des Arbeitgebers hergeleitet werden. Auch im Rahmen der nachvertraglichen Treuepflicht (Art. 321a Abs. 4 OR) fällt eine Löschung ausser Betracht, weil es sich gewöhnlich nicht um geheim zu haltende Tatsachen handelt.[64] Aus folgenden Gründen ist der Persönlichkeitsschutz des Arbeitnehmers (Art. 28 ff. ZGB) i. d. R. höher zu gewichten als die Ansprüche des Arbeitgebers: (a) die Kontaktdaten befinden sich auf einem Account im eigenen Namen, in welchen vom Arbeitnehmer (privat) investiert wird; (b) die Kontaktpersonen haben ihre Kontaktbestätigung oder die zuvor geschaltete Kontaktanfrage gegenüber der Person des Arbeitnehmers vorgenommen und nicht gegenüber der Person als blossem Vertreter des Arbeitgebers; (c) mit der Löschung würde in Rechtspositionen des Arbeitnehmers eingegriffen, weil sie ihn auch als individuelle Person betreffen würde.[65] Nach Beendigung des Arbeitsverhältnisses bleibt es dem Arbeitgeber in beiden Fällen jedoch unbenommen, sich gegen eine wettbewerbswidrige Verwendung der Kontaktdaten durch den ehemaligen Arbeitnehmer zur Wehr zu setzen.[66] Arbeitgebern ist zu *empfehlen,* ihre Arbeitnehmer proaktiv über die *Einrichtung entsprechender Unternehmens-Accounts* dazu zu bringen, über diese mit Geschäftskontakten zu kommunizieren. Es besteht dann die Möglichkeit, mittels eines Nutzungsreglements Einfluss auf das Verhalten des Arbeitnehmers zu nehmen, um insbesondere Probleme bei der Beendigung des Arbeitsverhältnisses zu vermeiden.

4. Screening von Stellenbewerbern

Das Internet kann eine ergiebige Quelle sein, um Informationen über Stellenbewerber zu beschaffen («Screening»). Grundsätzlich gilt, dass jede Datenerhebung und Datenbearbeitung einen *Arbeitsplatz-*

64 So auch ArbG Hamburg, Urteil vom 24. 1. 2013, Az. 29 Ga 2/13.

65 So Frik/Klühe (Fn. 60), S. 1176.

66 Siehe zur Typologie nachvertraglich unlauterer Verhaltensweisen Roger Rudolph, Kontakte zu Kunden des alten Arbeitgebers nach einem Stellenwechsel, ARV 2009, S. 93 ff., S. 102 f.

bezug braucht.[67] Denn gemäss Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur so weit bearbeiten, als sie das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsverhältnisses erforderlich sind. Dieser Grundsatz ist auch bezüglich Internetnutzung zu berücksichtigen und schützt potenzielle Arbeitnehmer im Bewerbungsverfahren.[68] Als Bearbeiten bezeichnet Art. 3 Bst. e DSG insbesondere das Beschaffen, Aufbewahren, Verwenden und Umarbeiten von Daten,[69] wobei der *rein gedankliche Umgang* nicht dazuzählt.[70] Man könnte somit argumentieren, dass das reine Googeln (d. h. die Suche des Arbeitgebers nach Informationen über einen Stellenbewerber im Internet) gemäss Art. 328b OR zulässig ist, sofern die Resultate nicht festgehalten, (intern) weitergegeben oder anderweitig verwendet werden.[71] Sobald die Suchergebnisse das Verhalten des Arbeitgebers gegenüber dem potenziellen Arbeitnehmer beeinflussen, ist hingegen von einer Datenbearbeitung im Sinne des DSG auszugehen.[72]

Art. 12 Abs. 3 DSG kann die Bearbeitung von Daten rechtfertigen, welche ohne Verbotsvorbehalt durch die betroffene Person selbst allgemein zugänglich gemacht wurden. Allerdings muss sich ein Arbeitgeber im Bewerbungsverfahren auch auf Informationen über den Stellenbewerber stützen können, welche Dritte im Internet bereitstel-

67 Streiff/von Kaenel/Rudolph (Fn. 13), Art. 328b N 5 und 6; von Kaenel (Fn. 13), S. 25 ff.; BSK OR I-Portmann/Rudolph (Fn. 40), Art. 328b N 8 f.

68 BGer 2C.103/2008 vom 21. 12. 2007, E. 6.2; Streiff/von Kaenel/Rudolph (Fn. 13), Art. 328b N 4, m. w. H.; von Kaenel (Fn. 13), S. 24. Teilweise a. M. Thomas Geiser, Darf die Arbeitgeberin den Bewerber googeln?, in: FS Schweizerischer Juristentag 2015, Zürich/St. Gallen 2015, S. 373 ff., S. 380 und 384; demnach soll bei Bewerbungen auf ausgeschriebene Stellen Art. 328 OR Anwendung finden, nicht aber bei Spontanbewerbungen.

69 Weiterführend zum «Umgang mit Personendaten» siehe Rosenthal/Jöhri (Fn. 39), Art. 3 N 63 ff.

70 Rosenthal/Jöhri (Fn. 39), Art. 3 N 69.

71 Im Ergebnis gl. M. Roberta Papa/Thomas Pietruszak, § 17 Datenschutz im Personalwesen, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht, Basel 2015, S. 577 ff., § 17.49; Geiser (Fn. 68), S. 384. A. M. für die Suche in privaten Netzwerken (z. B. Facebook) und im Internet allgemein («googeln»), da dort die Wahrscheinlichkeit, auf Informationen ohne Arbeitsplatzbezug zu treffen, sehr hoch sei: Stutz/Geiger-Steiner (Fn. 60), S. 213, Urs Egli, Soziale Netzwerke und Arbeitsverhältnisse, Jusletter vom 17. 1. 2011, Rz. 81 ff., Streiff/von Kaenel/Rudolph (Fn. 13) Art. 328b N 10.

72 Papa/Pietruszak (Fn. 71), § 17.49.

len.[73] Gleichzeitig bedarf der potenzielle Arbeitnehmer des Schutzes vor der Verwendung von Informationen ohne Arbeitsplatzbezug. Hier kommt Art. 328b OR zur Anwendung, der keine Beschränkung bezüglich des Ursprungs der Daten vorsieht, für die Datenbearbeitung aber einen Arbeitsplatzbezug voraussetzt. Dieser Bestimmung kommt eine selbständige Bedeutung neben dem DSG zu.[74] In Bewerbungsverfahren ist ihr deshalb Vorrang gegenüber Art. 12 Abs. 3 DSG zu geben.

Inwieweit ein *Bezug zum Arbeitsplatz* vorliegt, ist nach objektiven Kriterien in Bezug auf die konkrete Stelle zu beurteilen.[75] Unproblematisch dürften Informationen aus Business-Netzwerken (Xing oder LinkedIn) sein, da sie i. d. R. Auskunft über das geschäftliche Beziehungsnetz, bisherige Tätigkeiten und die Ausbildung des Arbeitnehmers geben.[76] Bei Datenerhebungen aus geschäftsfremden Internetquellen wie Google, Facebook, Twitter usw. kann nicht ohne Weiteres von einem Arbeitsplatzbezug ausgegangen werden. Für die Verwendung solcher Daten muss ein eindeutiger Bezug zur Eignung für das konkrete Arbeitsverhältnis vorliegen, ansonsten würde ihre Verwendung gegen Art. 328b OR verstossen. Nichtsdestotrotz erscheint z. B. das Googeln von Bewerbern heute als allgemein üblich.[77] Denn eine unzulässige Datenerhebung wird für den Arbeitgeber nur selten *rechtliche Konsequenzen* haben. So erhält der Arbeitnehmer i. d. R. gar keine Kenntnis von der missbräuchlichen Datenbearbeitung. Falls doch, stehen ihm kaum taugliche Rechtsbehelfe zur Verfügung, um sich dagegen zur Wehr zu setzen.[78] Und selbst wenn der Stellenbewerber ein unrechtmässiges Vorgehen nachweisen kann, wird er die angestrebte Anstellung nicht erhalten. Damit zielt die Schutzfunktion von Art. 328b OR in diesem Zusammenhang oftmals ins Leere.

73 Z. B. Listen von Ausbildungsstätten über ihre Absolventen, Informationen auf dem Internetauftritt des bisherigen Arbeitgebers, Beiträge in Onlinemedien usw.

74 VON KAENEL (Fn. 13), S. 43 f.

75 STREIFF/VON KAENEL/RUDOLPH (Fn. 13), Art. 328b N 5.

76 Folgende Autoren stellen zusätzlich auf die Zustimmung des Arbeitnehmers ab und kommen zum selben Ergebnis: PAPA/PIETRUSZAK (Fn. 71), § 17.48; STUTZ/GEIGER-STEINER (Fn. 60), S. 213; EGLI (Fn. 71), Rz. 65 ff.; STREIFF/VON KAENEL/RUDOLPH (Fn. 13), Art. 328b N 9; STUTZ/VALLONI (Fn. 27), S. 163.

77 PAPA/PIETRUSZAK (Fn. 71), § 17.49.

78 Ausführlich zu möglichen Rechtsbehelfen STREIFF/VON KAENEL/RUDOLPH (Fn. 13), Art. 328b N 19. A. M. CHRISTIAN FLUECKIGER, La googleisation des employés respecte-t-elle les principes de la protection des donnés?, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf/Zürich/Basel 2014, S. 73 ff., S. 94.

Es obliegt dem *Stellenbewerber, präventiv tätig zu werden.* Zunächst ist im Internet mit persönlichen Informationen haushälterisch umzugehen und das Hochladen problematischer Inhalte generell zu vermeiden. Mittels Privatsphäre-Einstellungen kann der (öffentliche) Zugang zu Daten auf Social-Media-Plattformen eingeschränkt werden. Kritische Internetinhalte können gegebenenfalls gelöscht werden.[79] Ist keine Löschung möglich, kann der Stellenbewerber versuchen, nachteilige Suchresultate zu verbessern oder mittels unverfänglicher Informationen zu verdrängen.[80] Verfehlen diese Massnahmen ihr Ziel, kann es angezeigt sein, nachteilige Internetfundstellen in der Bewerbung offen anzusprechen und kurz zu erklären. *Arbeitgeber sollten Aufmerksamkeit darauf verwenden,* beim Googeln von Stellenbewerbern oder Arbeitnehmern und beim Festhalten von Resultaten immer auf in der Stellenausschreibung beschriebene objektive Kriterien abzustellen. Alle objektiven Gründe, welche für Anstellungs- oder Kündigungsentscheidungen relevant sind, sollten dokumentiert werden.

IV. Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) bezeichnet die mit dem Arbeitgeber vereinbarte oder mit dessen stillschweigenden Einvernehmen erfolgende geschäftliche Nutzung eines privaten technischen Gerätes (meist Smartphone, Laptop, Tablet) durch den Arbeitnehmer.[81] Die Geräte stehen im Eigentum des jeweiligen Arbeitnehmers. Die Arbeitgeber erhoffen sich die bessere Erreichbarkeit ausserhalb der Arbeitszeiten, grössere Effizienz des Arbeitnehmers infolge Kenntnis

79 So wurde ein Löschungsanspruch für Bilder in Google Street View u. a. aufgrund des Rechts auf informationelle Selbstbestimmung in BGE 138 II 346 E. 8.2 anerkannt; vgl. zudem zum Recht auf Vergessen, EuGH vom 13. 5. 2014, Rs. C-131/12, Google. Bei Google kann die Löschung von Suchresultaten beantragt werden, siehe dazu das Formular unter <https://support.google.com/legal/contact/lr_eudpa?product=websearch>.

80 Die vorstehenden und weitere Massnahmen werden von verschiedenen Dienstleistungsunternehmen im Rahmen des Onlinereputationsmanagements angeboten.

81 Näheres zum Begriff Sébastien Fanti, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 165 ff., S. 166; Isabelle Conrad/Jochen Schneider, Einsatz von «privater IT» im Unternehmen, Zeitschrift für Datenschutz 2011, S. 153 ff., S. 153.

seines Gerätes sowie Kosteneinsparung bei Geräteanschaffungen. Den Arbeitnehmer trifft *keine Pflicht zu BYOD,* denn der Arbeitgeber hat die notwendigen Arbeitsgeräte grundsätzlich zur Verfügung zu stellen (Art. 327 Abs. 1 OR).[82] Aufgrund des Weisungsrechts des Arbeitgebers (Art. 321d OR) hat der Arbeitnehmer aber auch *kein Recht auf BYOD.*[83] Da sich aus BYOD verschiedene rechtliche Probleme ergeben können (nachfolgend unter 1., 2. und 3.), ist Arbeitgebern, die dieses Prinzip einführen oder dulden, dringend zu raten, BYOD in einem *Reglement* oder mit einer entsprechenden *Vereinbarung* mit den betreffenden Arbeitnehmern zu regeln.[84] Dabei ist auf eine strikte Trennung von privaten und geschäftlichen Daten zu achten.

1. Kostenteilung

Der Arbeitgeber hat arbeitsbegründete, notwendige Arbeitnehmerauslagen zu ersetzen (Art. 327a OR). Unbestritten ist die Entschädigungspflicht der geschäftsmässig begründeten *Verbindungskosten* (Telefon-/Internetgebühren) durch den Arbeitgeber. Hinsichtlich der *Abonnementskosten* dürfte eine Kostenbeteiligung angemessen sein, welche sich nach dem Anteil der geschäftlich begründeten Verwendung an der Gesamtnutzung richtet. Eine entsprechende Kostenteilung ist für *Anschaffungs- bzw. Amortisations- oder Reparaturkosten* ebenfalls denkbar.[85] Weil die Erhebung der privaten im Verhältnis zur

82 Holenstein (Fn. 6), S. 50; Fanti (Fn. 81), S. 171; Stutz/Valloni (Fn. 27), S. 177.

83 Reutter/Klaus (Fn. 26), S. 161.

84 Fanti (Fn. 81) S. 200; Reutter/Klaus (Fn. 26), S. 165; Nicole Beranek Zanon, Bring your own device (BYOD) aus rechtlicher Sicht, Jusletter IT vom 12. 9. 2012, Rz. 51 f. Siehe auch die Formulierungsbeispiele in Nicolas Birkhäuser/Marcel Hadorn, BYOD – Private Smartphones im geschäftlichen Arbeitsumfeld, SJZ 2013, S. 201 ff., S. 206; Stutz/Valloni (Fn. 27), S. 185.

85 Ebenso Birkhäuser/Hadorn (Fn. 84), S. 201. Einige Autoren (Fanti [Fn. 81], S. 178 f.; Reutter/Klaus [Fn. 26], S. 162; Stutz/Valloni [Fn. 27], S. 178 f.) knüpfen diesbezüglich an Art. 327b OR an, welcher Motorfahrzeuge betrifft. In der Regel dürften sich die hier besprochenen elektronischen Geräte deutlich von den Charakteristika eines Motorfahrzeuges unterscheiden (insb. hinsichtlich Preis, Unterhalt und Werthaltigkeit), weshalb die analoge Anwendung von Art. 327b OR auf BYOD nicht in Frage kommen kann.

geschäftlichen Nutzungsdauer problematisch sein dürfte, scheint die Vereinbarung einer monatlichen *Pauschalentschädigung* (Art. 327a Abs. 2 OR), welche die vorgenannten Ausgabestellen ausdrücklich berücksichtigt und den Arbeitnehmer tendenziell begünstigt, wohl am praktikabelsten zu sein.

2. Zugang des Arbeitgebers zum BYOD-Gerät

Da der Arbeitnehmer Eigentümer des BYOD-Gerätes ist, verliert der Arbeitgeber die Kontrolle über die Daten, was insbesondere bei Austritt aus dem Unternehmen oder bei Verlust und Diebstahl des Gerätes relevant sein kann. Für den Arbeitgeber ist es zentral, *Daten auf dem BYOD-Gerät zu bearbeiten* (z. B. durchsuchen oder löschen), um Sicherheits- und Reputationsrisiken einzudämmen.[86] Dafür ist allerdings ein *Rechtfertigungsgrund* notwendig, da es sich bei den betroffenen Daten zunächst um Personendaten des Arbeitnehmers im Sinne von Art. 2 Abs. 1 Bst. a DSG handelt. In diesem Zusammenhang ist im Sinne von Art. 328b OR zwischen privaten und geschäftlichen Personendaten zu unterscheiden. Der Arbeitnehmer kann der Bearbeitung geschäftlicher Personendaten (z. B. geschäftliche E-Mails) in einer generellen *Einwilligung,* z. B. im Rahmen einer BYOD-Vereinbarung, zustimmen. Eine stillschweigende Einwilligung des Arbeitnehmers wird vermutet bei geschäftlichen Daten, die der Arbeitnehmer mit anderen Mitarbeitern des Arbeitgebers teilt (vgl. Art. 12 Abs. 3 DSG). Demgegenüber bedarf es aufgrund der einseitigen Unabänderlichkeit von Art. 328b OR zum Nachteil des Arbeitnehmers (basierend auf Art. 362 Abs. 1 OR) jeweils einer fallweisen Zustimmung für eine Bearbeitung privater Daten. Anstelle einer Einwilligung kann ein *überwiegendes Interesse des Arbeitgebers* treten (Art. 13 Abs. 1 DSG). Im Fall des Verlusts des Gerätes oder bei Beendigung des Arbeitsverhältnisses kann beispielsweise eine Löschung der Daten im überwiegenden Interesse des Arbeitgebers liegen.[87] Ein überwiegen-

86 Vgl. zu Sicherheitsrisiken ROLAND PORTMANN, Private Smartphones im Geschäftsumfeld, digma 2012, S. 42 ff., S. 43; ANDREAS KOHNE/SONJA RINGLEB/CENGIZHAN YÜCEL, Bring your own Device, Wiesbaden 2015, S. 133 ff.

87 Ohne Rechtfertigungsgrund kann insbesondere auch Art. 144bis StGB (Datenbeschädigung) zur Anwendung kommen, siehe dazu FANTI (Fn. 81), S. 194 f.

des Interesse könnte ebenfalls bei der Durchsuchung von Daten infolge eines vermuteten schweren Missbrauchs (z. B. Straftat gegen den Arbeitgeber) vorliegen.

Jede Massnahme des Arbeitgebers steht jedoch unter der Bedingung, dass sie verhältnismässig (Art. 4 Abs. 2 DSG) ist. Ebenso muss der Arbeitnehmer bei einer allgemeinen Einwilligung (z. B. im Rahmen einer BYOD-Vereinbarung) darüber informiert worden sein, in welchen Fällen Daten bearbeitet bzw. gelöscht werden können (Ersichtlichkeit und Erkennbarkeit gem. Art. 4 Abs. 2 und 3 DSG). Gleichzeitig ist dem Arbeitnehmer die Datenbearbeitung anzukündigen, sofern kein berechtigtes Interesse (z. B. an einer verdeckten Untersuchung) entgegensteht (Prinzip von Treu und Glauben in Art. 4 Abs. 2 DSG). Zum *Einzug des BYOD-Gerätes* (ohne Bearbeitung der darauf befindlichen Daten) ist der Arbeitgeber berechtigt, falls der Arbeitnehmer in einer allgemeinen BYOD-Vereinbarung oder im Einzelfall zugestimmt hat.[88] Allerdings kann der Arbeitgeber in diesem Fall verpflichtet sein, den Arbeitnehmer dafür zu entschädigen oder für einen gleichwertigen Ersatz zu sorgen.[89]

3. Widersprüche zum Arbeitsgesetz (ArG)

Das Konzept des BYOD begünstigt den Trend zu einer «Entgrenzung» der Arbeit im Sinne der Aufhebung klarer Grenzen zwischen Wohn- und Arbeitsort und zwischen Arbeits- und Freizeit. Die ständige Erreichbarkeit kann im Konflikt mit den Bestimmungen zur zulässigen Höchstarbeitszeit und zur Nacht- und Sonntagsarbeit, zum Ferienbezug und zur Entlohnung stehen.[90] Durch den jederzeit möglichen Einsatz von BYOD-Geräten ist auch die Arbeitszeiterfas-

88 Zur Löschung, Durchsuchung oder Beschlagnahmung von BYOD-Geräten siehe Birkhäuser/Hadorn (Fn. 84), S. 202 ff.

89 Eine solche Pflicht kann für die geschäftliche Nutzung aus Art. 327 OR, wonach der Arbeitgeber verpflichtet ist, die notwendigen Arbeitsgeräte zur Verfügung zu stellen, und für die private Verwendung aus Art. 328 Abs. 1 OR, der Fürsorgepflicht des Arbeitgebers, abgeleitet werden.

90 Dunand (Fn. 4), S. 51; Fanti (Fn. 81), S. 172 ff. Weiterführend Adrian von Kaenel, Die ständige Erreichbarkeit des Arbeitnehmers, ARV 2009, S. 1 ff.

sung[91] durch den Arbeitgeber erschwert, was verwaltungsrechtliche Konsequenzen haben kann. Ausserdem kann der Arbeitgeber dadurch seine Fürsorgepflicht (Art. 328 OR) verletzen, welche im Anwendungsbereich des Arbeitsgesetzes in Art. 6 ArG sowie ArGV 3 konkretisiert wird.[92]

V. Elektronische Überwachung der Internetnutzung

Arbeitgeber sollen Arbeitnehmer identifizieren und zur Verantwortung ziehen können, falls diese die Regeln der Internet- und E-Mail-Nutzung am Arbeitsplatz verletzt haben oder entsprechende konkrete Anzeichen hierfür bestehen. Grundsätzlich gilt, dass Massnahmen der elektronischen Überwachung[93] der Internetnutzung *sehr strengen Voraussetzungen* unterliegen (nachfolgend unter 1.). Zulässig sind technische Massnahmen, die nicht personenbezogen ausgewertet werden können (z. B. Kontrolle Datenmenge, Filter, Sperrung bestimmter Websites).[94] Hingegen sind personenbezogene Kontrollen Datenbearbeitungen, die den strengen Bedingungen von Art. 328b OR, dem DSG und Art. 26 ArGV 3 genügen müssen. Zur elektronischen Überwachung der Internetnutzung gibt es derzeit einige aktuelle Fälle in der Rechtsprechung (nachfolgend unter 2.)

91 Diesbezüglich bringen die zwei neuen Ausnahmen zur systematischen Arbeitszeiterfassungspflicht, welche mit Art. 73a und 73b ArGV 1 am 1. 1. 2016 eingeführt wurden, gewisse Erleichterungen. So können Sozialpartner in einem Gesamtarbeitsvertrag vereinbaren, auf eine Arbeitszeiterfassung nach Massgabe der Verordnung zu verzichten (Art. 73a ArGV 1). Zudem ermöglicht Art. 73b ArGV 1 Vereinbarungen über eine vereinfachte Arbeitszeiterfassung.

92 Der Arbeitgeber muss aktiv Massnahmen zum Schutz der Arbeitnehmer treffen (Art. 328 Abs. 2 OR sowie Art. 6 Abs. 1 bis 2 ArG), insbesondere vor Gesundheitsgefährdung durch Überbeanspruchung (Art. 6 Abs. 2 ArG). Solche Massnahmen können die Information und Sensibilisierung der Arbeitnehmer sein oder aber auch technische Vorkehrungen, welche bewirken, dass geschäftliche Daten (z. B. E-Mails und Telefonate) ausserhalb der Arbeitszeit und während der Ferien nicht an das BYOD-Gerät weitergeleitet werden. Vgl. Thomas Letsch, Rechtliche Aspekte von Work-Life-Balance, Bern 2008, N 112 ff., N 123 ff. und N 133 ff.

93 Zu den verschiedenen Internet- und E-Mail-Überwachungsmöglichkeiten siehe Simon Wolfer, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsrechtsverhältnis, Zürich 2008, Rz. 474 ff.

94 Weiterführend zu den technischen Massnahmen Wolfer (Fn. 93), Rz. 490 f.

1. Grundsätze des DSG und des Art. 26 ArGV 3

Beim Surfen und Mailen werden an verschiedenen Orten Spuren hinterlassen. I. d. R. führen gemeinsam benutzte Informatikmittel wie Server eine Protokollierung der durchgeführten Aktivitäten durch. Sie erstellen sog. *Logfiles,* welche gemäss DSG Personendaten sind.[95]

Gemäss den *Grundsätzen des DSG* bedarf eine Datenbearbeitung eines Rechtfertigungsgrundes (Art. 13 Abs. 1 DSG) und muss den Grundsatz der Verhältnismässigkeit wahren (Art. 4 Abs. 2 DSG). Dies bedeutet, dass nur diejenigen Auswertungen vorgenommen werden dürfen, die für das Aufdecken von Missbräuchen geeignet sind. Dabei hat der Arbeitgeber diejenige Auswertungsform zu wählen, welche den mildesten Eingriff in die Persönlichkeitsrechte des Arbeitnehmers darstellt.[96] Der Grundsatz der Zweckbindung nach Art. 4 Abs. 3 DSG bedeutet, dass die Logfiles nur für diejenigen Zwecke verwendet werden dürfen, welche den Arbeitnehmern bekannt gegeben wurden. Diesem Grundsatz kommt der Arbeitgeber durch den Erlass eines Nutzungsreglements und durch die regelkonforme Datenbearbeitung nach. Im Nutzungsreglement muss festgehalten werden, welche Auswertungen für welche Zwecke mit welchen Daten (Logfiles) durchgeführt werden. Die Notwendigkeit des Erlasses eines Nutzungsreglements ergibt sich aus dem Grundsatz der Transparenz.[97]

Der Gesundheitsschutz des Arbeitnehmers beim Einsatz von Überwachungs- und Kontrollsystemen wird in *Art. 26 ArGV 3* geregelt. Gemäss der Rechtsprechung des Bundesgerichts zu Art. 26 Abs. 1 ArGV 3 ist es verboten, das Verhalten der Arbeitnehmer zu überwachen, sofern sich die Überwachung negativ auf die Gesundheit oder das Wohlbefinden des Arbeitnehmers auswirken kann.[98] Dies ist insbesondere dann

95 Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) über Internet- und E-Mail-Überwachung am Arbeitsplatz – Für die Privatwirtschaft, Sept. 2013, abrufbar unter: <www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html>, S. 4.

96 Leitfaden EDÖB (Fn. 95), S. 5; ArbGer ZH (Fn. 12), E. 5.2.1; Papa/Pietruszak (Fn. 71), § 17.49; Wolfer (Fn. 93), Rz. 67 f.

97 Leitfaden EDÖB (Fn. 95), S. 6; ArbGer ZH (Fn. 12), E. 5.2.1; Wolfer (Fn. 93), Rz. 493 f.; Papa/Pietruszak (Fn. 71), § 17.68.

98 Einschränkende Auslegung der Bestimmung in BGer 6B.536/2009 vom 12. 11. 2009, E. 3.6.1. f., bestätigt in BGer 9C.785/2010 vom 10. 6. 2011, E. 6.3 (beide zur Videoüberwachung des Kassenbereichs); Papa/Pietruszak (Fn. 71), § 17.55.

der Fall, wenn die Verhaltensüberwachung nicht nur sporadisch oder bei bestimmten Gelegenheiten stattfindet.[99] Werden Überwachungs- und Kontrollsysteme primär für andere Zwecke (z. B. aus Sicherheitsgründen) eingesetzt, so sind die zulässig, wenn sie so ausgestaltet sind, dass die Gesundheit und Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3).[100] Für das Surfen und Mailen am Arbeitsplatz bedeutet dies, dass die ständige personenbezogene Auswertung von Logdaten für die Überwachung des Nutzungsverhaltens grundsätzlich nicht zulässig ist.[101] In bestimmten Bereichen der Privatwirtschaft, z. B. bei den Banken, wird die systematische Überwachung und Auswertung indessen zu einer Voraussetzung, damit das Unternehmen die Compliance-Anforderungen erfüllen kann.[102]

Der Arbeitgeber darf, bei Beachtung des Grundsatzes der Verhältnismässigkeit und einer entsprechenden Transparenz gegenüber den Betroffenen, elektronische Spuren und Protokollierungen (z. B. Logfiles) zu Kontrollzwecken oder auch zur Missbrauchsprävention erstellen und bearbeiten.[103] Eine ständige personenbezogene Auswertung ist zwar nicht zulässig, jedoch darf eine personenbezogene namentliche Auswertung dann durchgeführt werden, wenn mindestens ein konkreter Missbrauchsverdacht besteht (z. B. ein beleidigendes «Posting») oder aufgrund einer personenbezogenen, nicht namentlichen Auswertung feststeht, dass es zu einem Missbrauch gekommen ist und nun die konkrete Person identifiziert werden soll.[104] Der Rechtfertigungsgrund der personenbezogenen Auswertung liegt im überwiegenden Interesse des Arbeitgebers an der Klärung des Sachverhalts und der Verantwortlichkeiten im Falle der Verletzung seiner Interessen.

99 BGer 9C.785/2010 vom 10. 6. 2011, E. 6.3; Papa/Pietruszak (Fn. 71), § 17.55.

100 Papa/Pietruszak (Fn. 71), § 17.55.

101 Giordano Costa, Internet- und E-Mail-Überwachung am Arbeitsplatz, Jusletter vom 9. 1. 2012; Thomas Geiser, Die Beaufsichtigung des Internetbenutzers im Arbeitsrecht, medialex 20/01, S. 201 ff.; Sylvain Métille, La surveillance électronique des employés, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 99 ff.; Aubert/Delley (Fn. 4), S. 148 ff., m. w. H.; Holenstein (Fn. 6), S. 94 ff; Papa/Pietruszak (Fn. 71), § 17.72.

102 Leitfaden EDÖB (Fn. 95), S. 5 f.; ArbGer ZH (Fn. 12), E. 5.2.2.

103 Urs Maurer-Lambrou/Andrea Steiner, in: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.), 3. Aufl., Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, Basel 2014, Art. 4 N 29.

104 Leitfaden EDÖB (Fn. 95), S. 9; ArbGer ZH (Fn. 12), E. 5.4.

2. Aktuelle Rechtsprechung

In einem *Entscheid des Obergerichts Zürich* vom März 2015 hatte eine Bank Logfiles, welche aus technischen und Compliance-rechtlichen Gründen zwingend vorhanden waren, auf einen konkreten Missbrauchsverdacht hin (ein anonym verfasster, beleidigender Kommentar auf der Website «Inside Paradeplatz») zulässigerweise ausgewertet.[105] Die geposteten Blog-Einträge des Arbeitnehmers stellten eine Treuepflichtverletzung gegenüber dem Arbeitgeber dar. Aufgrund der «Postings» bestand ein konkreter Missbrauchsverdacht gegenüber einem Arbeitnehmer. Eine personenbezogene Auswertung der Logfiles war daher zulässig, um die konkrete Person zu identifizieren. Das Vorgehen des Arbeitgebers war geeignet, den Missbrauch aufzudecken und den konkreten Arbeitnehmer zu identifizieren. Eine mildere Massnahme war nicht ersichtlich, sodass auch die Verhältnismässigkeit gegeben war. Eine allfällige Datenschutzverletzung müsste gemäss Zürcher Obergericht eine mit den gesetzlichen Missbrauchstatbeständen gemäss Art. 336 OR vergleichbare Schwere aufweisen, um eine im Gesetz nicht genannte Missbräuchlichkeit der Kündigung gestützt auf Art. 2 Abs. 2 ZGB begründen zu können.[106]

Hingegen hat das Bundesgericht in einem Entscheid vom Januar 2013, in *BGE 139 II 7,* entschieden, dass der verdeckte Einsatz eines Überwachungsprogrammes zwecks Bestätigung des Verdachts, ein Arbeitnehmer missbrauche die ihm im Informatikbereich zur Verfügung gestellten Mittel für dienstfremde Zwecke, unzulässig (Art. 26 Abs. 1 ArGV 3) oder zumindest unverhältnismässig (Art. 26 Abs. 2 ArGV 3) sei. Zwar stellten der Kampf gegen Missbrauch und die Kontrolle der Arbeitsleistung der Angestellten ohne Zweifel ein legitimes Interesse des Arbeitgebers dar. Diese Ziele könnten indessen auch mittels weniger eingreifender Mittel erreicht werden. Aufgrund der legalen Möglichkeiten eines Arbeitgebers, etwaige Missbräuche der Informatikanlage festzustellen und zu verfolgen, erklärte das Bundesgericht das rechtswidrig erlangte Beweismittel für im Prozess nicht verwertbar. Mit der Verneinung der Verwertbarkeit eines auf diese Weise widerrechtlich erlangten

105 OGer ZH (Fn. 12), E. 3.1.

106 OGer ZH (Fn. 12), E. 3.1; Streiff/Von Kaenel/Rudolph (Fn. 13), Art. 336 N 4.

Beweismittels falle aber auch die Grundlage für eine fristlose Kündigung dahin.

In einem (noch nicht rechtskräftigen) *Fall des Bundesverwaltungsgerichts vom Dezember 2015* ging es um die gerechtfertigte fristlose Entlassung zweier SBB-Angestellter, die während der Arbeitszeit bis zu vier Stunden täglich im Internet Pornos anschauten.[107] Das Tun der beiden Männer flog auf, weil der betriebsinterne Informatikdienst eine intensive Nutzung pornografischer Websites festgestellt und daraufhin nachträglich die Daten der zwei im Verdacht stehenden Mitarbeiter ausgewertet hatte. Das Bundesverwaltungsgericht kam in seinem Urteil zum Schluss, dass der Informatikdienst damit zwar nicht ganz den Buchstaben des Gesetzes entsprochen habe. Das Regierungs- und Verwaltungsorganisationsgesetz (RVOG) sieht in den am 1. April 2014 in Kraft getretenen Bestimmungen zur Bearbeitung von Personendaten bei der Nutzung elektronischer Infrastruktur nämlich vor, dass die Daten eines Mitarbeiters der erweiterten Bundesverwaltung wegen Verdachts auf Internetmissbrauch nur dann kontrolliert werden dürfen, wenn er vorher schriftlich informiert worden ist.[108] In den vorliegenden Fällen hatte die SBB dies unterlassen. Das Bundesverwaltungsgericht stellte fest, dass gewisse formelle Mängel bei den IT-Abklärungen vorlagen, dass diese aber nicht so schwer wogen, als dass der entsprechende Kontrollbericht nicht hätte verwendet werden dürfen.[109]

Mit einem (noch nicht rechtskräftigen) *Urteil vom 12. Januar 2016, Bărbulescu v. Romania, hat die Kammer des EGMR* festgestellt, dass die elektronische Überwachung der Internetnutzung eines Arbeitnehmers und dessen darauf gestützte Kündigung im konkreten Fall gerechtfertigt seien und nicht gegen Art. 8 EMRK verstiessen.[110] Auf Weisung des Arbeitgebers hatte Herr Bărbulescu, ein für den Verkauf verantwortlicher Ingenieur, einen Yahoo Messenger Account kreiert, um Anfragen von Klienten zu beantworten. Am 13. Juli 2007 wurde Herrn Bărbulescu mitgeteilt, dass seine Yahoo Messenger Kommunikation vom 5. bis 13. Juli 2007 überwacht worden sei und dass diese Überwachung gezeigt habe, dass er das Internet für private Zwecke

107 BVGer A-5641/2014 vom 8. 12. 2015 und A-6453/2014 vom 9. 12. 2015.

108 Art. 57o Abs. 2 lit. b RVOG zur namentlichen personenbezogenen Auswertung. Siehe dazu BVGer A-5641/2014 vom 8. 12. 2015, E. 5.2 bis 5.4.

109 BVGer A-5641/2014 vom 8. 12. 2015, E. 6 (mit Verweis auf Art. 152 ZPO).

110 EGMR, Kammerurteil vom 12. 1. 2016, Bărbulescu/Romania, Nr. 61496/08.

genutzt habe, nämlich für private Nachrichten an seinen Bruder und seine Verlobte zu seiner Gesundheit und seinem Sexleben. Am 1. August 2007 kündigte der Arbeitgeber den Arbeitsvertrag (unter Einhaltung der nationalen Kündigungsbestimmungen) wegen Verletzung der internen Weisungen, welche die Nutzung der IT-Infrastruktur für private Zwecke gänzlich verboten und dem Arbeitnehmer bekannt waren. Die Kammer des EGMR hielt fest, dass im vorliegenden Fall Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz) anwendbar sei (N 45). Die nationalen Behörden hätten (innerhalb ihres Ermessensspielraums) eine gerechte Abwägung zwischen Herrn Bărbulescus Recht auf Privatleben und Korrespondenz nach Art. 8 EMRK und den Interessen des Arbeitgebers vorgenommen, Art. 8 EMRK sei nicht verletzt (N 54–63). Aus diesem Urteil kann geschlossen werden, dass eine elektronische Überwachung, welche einen Eingriff in das Privatleben und die Korrespondenz des Arbeitnehmers bewirken kann, nicht per se unzulässig ist. Die elektronische Überwachung durch den Arbeitgeber kann im Kontext eines Disziplinar- bzw. Kündigungsverfahrens im Sinne von Art. 8 Abs. 2 EMRK gerechtfertigt sein, wofür die nationale Gesetzgebung und gewisse Voraussetzungen eingehalten werden müssen.[111]

VI. Nutzungsreglemente

1. **Regelungskompetenz des Arbeitgebers**

Gemäss Art. 321d Abs. 1 OR kann der Arbeitgeber allgemeine Anordnungen über die Ausführung der Arbeit und das Verhalten der Arbeitnehmer im Betrieb erlassen und ihnen besondere *Weisungen* erteilen. Gleichzeitig hat der Arbeitgeber gemäss Art. 328 Abs. 1 OR eine Fürsorgepflicht und muss die Persönlichkeit des Arbeitnehmers achten und schützen. Weisungen müssen deshalb grundsätzlich im direkten Zusammenhang mit der Einhaltung des Arbeitsvertrages stehen, das Persönlichkeitsrecht des Arbeitnehmers respektieren und dürfen den üblichen Rahmen nicht überschreiten.[112] Problematisch ist

111 Vgl. auch EGMR, Kammerurteil vom 3.4.2007, Copland/UK, Nr. 62617/00, N 47 f.

112 Ausführlich dazu HOLENSTEIN (Fn. 6), S. 30 ff.

die arbeitgeberseitige Regelung von *ausschliesslich privaten Nutzungen des Internets* oder von ausschliesslich privat genutzten Social-Media-Accounts.[113] Grundsätzlich können Arbeitgeber ihren Arbeitnehmern die private Internetnutzung nicht vorschreiben, und es besteht keine Regelungsbefugnis des Arbeitgebers. Solange das Verhalten keine Auswirkung auf das Arbeitsverhältnis hat, darf der Arbeitgeber das private Verhalten des Arbeitnehmers ausserhalb der Arbeitszeit weder einschränken noch untersagen noch arbeitsrechtlich sanktionieren. Die private Nutzung des Internets *während* der Arbeitszeit muss der Arbeitgeber hingegen nur beschränkt dulden. Der Arbeitgeber hat Interesse daran, dass der Arbeitnehmer keine exzessive Nutzung des Internets während der Arbeitszeit betreibt, da dieser seine Pflicht zur Leistung von Arbeit gemäss Art. 319 Abs. 1 OR erfüllen soll.

Fehlt eine Anweisung des Arbeitgebers zur privaten Nutzung des Internets, gelten die gleichen Regelungen wie für die Nutzung von Telefons oder E-Mail, d. h., die Privatnutzung ist grundsätzlich zulässig, solange die Arbeitsleistung nicht gefährdet ist und das übliche Mass nicht überschritten wird.[114] Denn das Bundesgericht[115] und der EGMR[116] schützen dem Grundsatz nach den Anspruch des Arbeitnehmers, während der Arbeitszeit Privatangelegenheiten erledigen zu können. Das komplette Verbot jeder privaten Nutzung von E-Mail, Telefon oder Internet während der Arbeitszeit beeinträchtigt das in

113 Siehe dazu die Tabelle 3 von WILDHABER/HÄNSENBERGER (Fn. 9), S. 425; BORSUTZKY (Fn. 5), S. 648 ff; DUNAND (Fn. 4), S. 38 ff.

114 EGLI (Fn. 71), Rz. 36, 42, 48; AUBERT/DELLEY (Fn. 4), S. 154; HOLENSTEIN (Fn. 6), S. 47, S. 82; STREIFF/VON KAENEL/RUDOLPH (Fn. 13), Art. 328b N 17; BRUNO BAERISWYL, 10 Jahre Datenschutz im Arbeitsrecht, in: Aktuelle Probleme des Arbeitsrechts, Zürich 2005, S. 51 ff., S. 62; BEAT RUDIN, Was darf die Chefin, was die Angestellte? Arbeits- und datenschutzrechtliche Schranken der technischen Überwachung der Internet-Nutzung am Arbeitsplatz, DIGMA 2001, S. 4 ff.; DUNAND (Fn. 8), S. 8 f.; GABRIEL AUBERT, Art. 319–362 CO, in: Commentaire romand Code des obligations I, Luc Thévenoz/Franz Werro (Hrsg.), 2. Aufl., Basel 2012, Art. 328b OR N 8.

115 BGer 4A.430/2008 vom 24. 11. 2008, E. 4.1.

116 EGMR, Urteil vom 16. 12. 1992, Niemietz/Deutschland, Nr. 13710/88; EGMR, Urteil vom 25. 6. 1997, Halford/Vereinigtes Königreich, Nr. 20605/92; EGMR, Urteil vom 3. 7. 2007, Copland/Vereinigtes Königreich, Nr. 62617/00; EGMR, Urteil vom 23. 9. 2010, Schüth/Deutschland, Nr. 1620/03; EGMR, Urteil vom 12. 6. 2014, Martinez/Spanien, Nr. 56030/07; KURT PÄRLI, Schutz der Privatsphäre am Arbeitsplatz in digitalen Zeiten, eine menschenrechtliche Herausforderung, EuZA 2015, S. 58 ff.

Art. 8 EMRK verankerte Recht auf Privatleben am Arbeitsplatz. Eine Verletzung der arbeitsvertraglichen Leistungspflicht wiegt umso schwerer, je mehr der Arbeitnehmer bei der privaten Nutzung des Internets seine Arbeitspflicht in zeitlicher und inhaltlicher Hinsicht vernachlässigt.[117] Es verbleibt offensichtlich ein grosser Unschärfebereich, wobei eben ein Nutzungsreglement Klarheit schaffen kann.

Die *Nutzung unternehmenseigener Infrastruktur* kann der Arbeitgeber umfassend regeln und einschränken. Somit kann er die private Nutzung des Internets auf seiner betrieblichen Infrastruktur einschränken oder ganz verbieten.[118] Es besteht in anderen Worten kein Anspruch auf die private Nutzung des Internets auf betrieblicher Infrastruktur. Insofern steht es dem Arbeitgeber frei, Arbeitnehmern den Zugang zu (gewissen) Websites zu sperren.[119] Ein gleichzeitiges Verbot privater Geräte (insbesondere Smartphones) am Arbeitsplatz hätte sich indessen nach den Voraussetzungen von Art. 8 EMRK zu richten.

2. Regelung durch Nutzungsreglemente

Arbeitgebern ist zu empfehlen, ihr Weisungsrecht zur Nutzung des Internets am Arbeitsplatz mittels eines Nutzungsreglements zu regeln.[120] Die Arbeitnehmer sind sich der Folgen ihres Verhaltens im Internet (z. B. auf Social-Media-Plattformen) oft nicht vollumfänglich bewusst.[121] Deshalb ist es sinnvoll, sie bezüglich ihres Verhaltens im Netz zu *sensibilisieren*. Regelungen zuhanden des Arbeitgebers sollten nicht nur die Zulässigkeit und die Begrenzung der Nutzung des

117 Vgl. DUNAND (Fn. 4), S. 41 f, m. w. H.

118 Allgemein zum Weisungsrecht des Arbeitgebers, private Nutzung auf betrieblichen Geräten zu verbieten: BGer 4A.430/2008 vom 24. 11. 2008, E. 4.1; STUTZ/GEIGER-STEINER (Fn. 60), S. 214; EGLI (Fn. 71), Rz. 33; DUNAND (Fn. 4), S. 40; ALDER (Fn. 4), S. 277. Kritisch zu einem generellen Verbot REINHARD OERTLI, Internet am Arbeitsplatz – Ein informationsrechtlicher Streifzug, in: FS Jean Nicolas Druey, Zürich 2002, S. 894 ff. (widerspräche dem Persönlichkeitsrecht des Arbeitnehmers).

119 STUTZ/GEIGER-STEINER (Fn. 60), S. 214; EGLI (Fn. 71), Rz. 33.

120 DOMINIK MARBET/RENÉ PFISTER, Soziale Netzwerke (Social Media) – Richtlinien: Worauf Arbeitgeber und Arbeitnehmende achten sollten, Schweizer Arbeitgeber 2011, S. 17 f.

121 OBERWETTER (Fn. 62), S. 420; BYERS/MÖSSNER (Fn. 8), S. 1666.

Internets, sondern auch Handlungsvorgaben zu einem verantwortungsvollen Umgang mit dem Internet beinhalten.[122] Sie können ebenfalls dazu dienen, unverbindliche *Handlungsempfehlungen* für den privaten Bereich zu geben. So kann hinsichtlich einer verantwortungsbewussten Nutzung im Privatbereich sensibilisiert werden, ohne dass unzulässig in das Recht auf freie Meinungsäusserung eingegriffen wird (z. B. durch den unverbindlichen Hinweis, wonach sich kritische Äusserungen im Privatbereich schädlich für das Unternehmen auswirken können). Dadurch können mögliche Konfliktsituationen vermieden werden, bevor sie entstehen.

Erlässt der Arbeitgeber keine Nutzungsregeln, kann ihm vorgeworfen werden, dass er nicht genügend Massnahmen gegen einen möglichen Missbrauch der Nutzung von elektronischen Kommunikationsmitteln ergriffen hat, weshalb eine personenbezogene Überwachung und Kontrolle der Internetaktivitäten seiner Arbeitnehmer von Vornherein ausgeschlossen sein kann, da sie nicht *verhältnismässig* (Art. 4 Abs. 2 DSG) ist. Die Erforderlichkeit der Massnahme ist bei fehlender individueller Vereinbarung oder Anordnung kaum gegeben, da eine gleich geeignete, aber mildere Massnahme, nämlich der Erlass einer Nutzungsregelung, für den angestrebten Erfolg zumeist ausreichen würde.

Die Regelung der Nutzung des Internets wirkt sich somit unmittelbar auf die *Kontrollrechte* des Arbeitgebers aus. Ist die Nutzung des Internets am Arbeitsplatz grundsätzlich verboten oder mindestens beschränkt, hat der Arbeitgeber das Recht, die Einhaltung seiner Weisung – unter gewissen datenschutzrechtlichen (z. B. Art. 26 ArGV 3) und arbeitsgesetzlichen Einschränkungen – auch zu kontrollieren.[123] Ist die Nutzung des Internets hingegen nicht reglementiert oder erlaubt, sind Kontrollen nur zulässig, wenn konkrete Hinweise auf eine Verletzung der Treuepflicht durch den Arbeitnehmer bestehen oder sich die Notwendigkeit des Zugriffs auf geschäftliche Daten (z. B. bei

122 Paul Melot de Beauregard/Christian Gleich, Social Media am Arbeitsplatz – Chancen und Risiken, DB 2012, S. 2044 ff., S. 2045.

123 Betreffend Überwachungsmassnahmen in engen Grenzen vgl. Leitfaden EDÖB (Fn. 95); von Kaenel (Fn. 13), S. 43 f.; BGE 139 III 7. Siehe auch den Fall «Inside Paradeplatz» (Fn. 12), wo die Bank als Arbeitgeberin geltend machte, die IT-Nutzung sowie die Ausübung von Kontrollrechten seien durch ein vom Arbeitnehmer akzeptiertes Überwachungsreglement abgestützt.

BYOD) ergibt.[124] Immer unzulässig ist das Eindringen in Inhalte, die anlässlich einer Kontrolle als privat erkannt wurden.

VII. Schlusswort

Bei der Nutzung von Internet am Arbeitsplatz stellt sich für die Rechtspraxis die grosse Herausforderung, zwischen den berechtigten Interessen der Arbeitnehmer und Arbeitgeber abzuwägen. Es empfiehlt sich die Einführung eines Nutzungsreglements, um Unklarheiten bezüglich Nutzung von Internet, E-Mail und Social Media, bezüglich Schutzes vor Persönlichkeitsverletzungen, bezüglich BYOD und der elektronischen Überwachung am Arbeitsplatz zu regeln. Ein solches Nutzungsreglement hilft sowohl dem Arbeitgeber als auch den Arbeitnehmern, eine klare Grenze zwischen Arbeit und Privatem zu ziehen und Transparenz zu schaffen.

124 Streiff/von Kaenel/Rudolph (Fn. 13), Art. 328b N 18; von Kaenel (Fn. 13), S. 44 f. Siehe auch den Fall «Inside Paradeplatz» (Fn. 12), wo die Bank als Arbeitgeberin geltend machte, dass bei konkretem Verdacht einer rechtlich relevanten Pflichtverletzung ein Kontrollrecht bestehe.