Rechtliche Risiken von sozialen Medien im Rahmen des Arbeitsverhältnisses

Mirjam Zai

Studiengang: MAS HR & Recht

Rechtliche Risiken von sozialen Medien im Rahmen des Arbeitsverhältnisses

Masterthesis

ZHAW Zürcher Hochschule für Angewandte Wissenschaften
School of Management and Law

Eingereicht bei: Dr. Urs Egli, Hauptreferent
Dr. Nicole Vögeli Galli, Korreferentin

Vorgelegt von: Mirjam Zai
Studiengang: MAS HR & Recht

8. November 2022

Wahrheitserklärung

Hiermit erkläre ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Masterarbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch die Angaben der Herkunft kenntlich gemacht. Ich versichere zudem, diese Arbeit nicht bereits anderweitig als Leistungsnachweis verwendet zu haben.

8. November 2022

_____

Mirjam Zai

Management Summary

Soziale Medien haben sich in den letzten Jahren im privaten Bereich wie auch in der Geschäftswelt als einen festen Bestandteil in der digitalen Kommunikation etabliert. Arbeitgebende und Mitarbeitende nutzen soziale Medien immer häufiger aus unterschiedlichen Gründen. Durch die Nutzung von sozialen Medien sind beide Seiten verschiedenen Risiken ausgesetzt. Deren Folgen reichen von Streitereien über Eigentumsverhältnisse und Arbeitszeitnutzung, Shitstorms, Cyberangriffen bis hin zu existenzbedrohenden Imageschädigungen für Unternehmen.

Diese Masterthesis untersucht, wo die rechtlichen Risiken im Arbeitsverhältnis bei der Nutzung von sozialen Medien liegen und wie Arbeitgeber diesen am effektivsten begegnen. Um die Forschungsfragen zu beantworten, wurden die Risikofelder im Internet recherchiert. Danach erfolgte für die einzelnen Themen eine Gesetzes-, Literatur- und Urteilsanalyse.

Die Thesis zeigt auf, dass die Problematiken sehr vielfältig sind. Gewisse Themen sind altbekannt und haben auch in der digitalen Welt Nährboden gefunden. Andere Risiken sind erst durch die Digitalisierung und Nutzung von sozialen Medien entstanden. Insbesondere die Themenbereiche Datenschutz, Persönlichkeitsschutz, Treuepflicht sowie Geheimhaltungspflicht werden durch die Nutzung von sozialen Medien tangiert. Für Arbeitgeber sind speziell die rechtlichen Rahmenbedingungen in Bezug auf Überwachungsmassnahmen sowie Sanktionen von Bedeutung. Mit dem Straf-, Urheber-, Gleichstellungs-, Datenschutz- sowie dem Wettbewerbsrecht sind auch weitere Rechtsgebiete in die komplexe Thematik der Social-Media-Nutzung im Arbeitsverhältnis eingebunden. Für Arbeitgeber lohnt es sich kaum, bei Konflikten den Rechtsweg zu beschreiten. Faktoren wie finanzieller und zeitlicher Aufwand, beschränkter Schadenersatz sowie Unklarheiten in Bezug auf die Rechtsauslegung spielen dabei eine Rolle.

Entsprechend ist der Fokus von Unternehmen auf Präventivmassnahmen zu setzen, um die verschiedenen Risiken zu minimieren. Insbesondere die Sensibilisierung der Mitarbeitenden in Bezug auf die vielfältigen Fallstricke sowie die Erstellung von Social-Media-Richtlinien sind zu empfehlen. Dabei einher geht auch dich Entwicklung der Social-Media-Kompetenz der Mitarbeitenden. Die Masterthesis zeigt auf, dass die digitale Entwicklung und der Faktor Mensch zu vielseitigen Herausforderungen an der Schnittstelle von Personalmanagement und Arbeitsrecht führen.

Inhaltsverzeichnis

.

Glossar

Account	Konto eines Nutzers für ein Dienstleistungsangebot in einem Computernetzwerk.
Active Sourcing	Konzept in der Personalbeschaffung, bei welchem die Unternehmen aktiv Kontakt mit potenziellen Bewerbenden aufbauen.
Awareness-Aktion	Sensibilisierung der Mitarbeitenden in Bezug auf das Sicherheitsbewusstsein.
Big Data	Grosse Mengen an Daten, die aus Bereichen wie Internet und sozialen Medien stammen und die mit speziellen Lösungen gespeichert, verarbeitet und ausgewertet werden.
Code of Conduct	Sammlung von Richtlinien/Regelungen, welche sich Unternehmen im Rahmen einer freiwilligen Selbstbindung auferlegen.
Compliance	Einhaltung von Gesetzen, Regeln und Normen.
Content Creator	Medienschaffender, der multimediale Inhalte entwickelt.
Corporate Design	Visuelles Erscheinungsbild eines Unternehmens.
Corporate Influencer	s. Kapitel 2.9.3.
Corporate Language	Individueller und charakterisierender Sprachstil und -gebrauch eines Unternehmens.
Cyberangriff	Angriff von aussen auf eine IT-Infrastruktur zur Sabotage, Informationsgewinnung und Erpressung.
Cybermobbing	Verschiedene Formen der Verleumdung, Belästigung, Bedrängung und Nötigung anderer Menschen mit Hilfe elektronischer Kommunikationsmittel.
Domain	Gliederungseinheit im Internet bezüglich der hierarchisch aufgebauten Rechnernamen.
Download	Arbeitsprozess, bei dem ein Datenfluss von einem Netzbetreiber oder dem Internet zum Endgerät eines Nutzers stattfindet.
Early Adopters	Personen, die die neuesten technischen Errungenschaften oder die neuesten Varianten von Produkten nutzen.
Employee Advocacy	s. Kapitel 2.9.3.

Employee Lifecycle	Laufbahn eines Angestellten innerhalb eines Unternehmens, vom Recruiting über die Einstellung bis hin zum Ausscheiden.
Employer Branding	Aufbau und Pflege der Arbeitgebermarke.
Fake News	Falsch- und Fehlinformationen, die häufig über elektronische Kanäle verbreitet werden.
Firewall	Hard- und Software, um den Zugriff auf Rechner von aussen durch unbefugte Dritte zu verhindern und so interne Daten zu schützen.
Follower	Internetnutzer, die anderen Internetnutzern auf sozialen Netzwerken folgen.
GPS-System	Globales Navigationssatellitensystem zur Positionsbestimmung.
Influencer	Personen, die in den sozialen Medien eine grosse Reichweite und einen hohen Bekanntheitsgrad haben.
IP-Adresse	Eindeutige Adresse eines Rechners oder eines Internetservers innerhalb eines Netzwerks.
Liken	Nutzer sozialer Netzwerke bringen per Auswahlfeld zum Ausdruck, dass ihnen etwas gefällt oder sie etwas unterstützen.
Logdaten/Logfile	Datei in der alle bzw. zuvor definierte Aktionen und Ereignisse eines Systems protokolliert werden.
Metaverse	Digitaler Raum, der durch das Zusammenwirken von virtueller, erweiterter und physischer Realität entsteht.
Multi-Faktor-Authentifizierung	Prozess der Account-Sicherheit, der zwei oder mehrere separate Schritte erfordert, damit ein Benutzer seine Identität nachweisen kann.
Onboarding	Das Einstellen neuer Mitarbeiter sowie alle Massnahmen, welche die Integration im Unternehmen fördern.
People Analytics	s. Kapitel 2.2.6.
Phishing	Abfangen von Daten von Internetnutzern über gefälschte Internetadressen, E-Mails etc.
Post/Posting	Beitrag auf einer Social-Media-Plattform.
Retweet	Weiterleiten einer bereits durch andere Nutzer veröffentlichten Nachricht oder Statusmeldung auf Twitter an die eigenen Follower.

Robot Recruiting	Verwendung künstlicher intelligenter Systeme im Bereich der Personalbeschaffung.
Screening	Systematische Prüfverfahren
Screenshot	Abbildung des Bildschirminhalts oder eines Teils davon.
Share Button	Funktion für das Teilen/Weiterverbreiten von Seiten in den sozialen Netzwerken.
Shitstorm	Sturm der Entrüstung im virtuellen Raum, in sozialen Medien, sowie in Kommentarbereichen von Onlinemedien.
Social Media	Digitale Plattformen, die es Nutzern ermöglichen, sich im Internet zu vernetzen, untereinander auszutauschen und mediale Inhalte einzeln, in einer definierten Gemeinschaft oder offen in der Gesellschaft zu erstellen und weiterzugeben.
Social-Media-Coaches	Berater für den Umgang mit sozialen Medien.
Social-Media-Monitoring	Durchsuchen der sozialen Medien nach Informationen und Nutzerprofilen, die für ein Unternehmen relevant sind.
Spam	Unerwünschte, in der Regel auf elektronischem Weg übertragene massenhafte Nachrichten, die dem Empfänger unverlangt zugestellt werden.
Spyware	Software, die sich versteckt, unbemerkt Daten erfasst und die Online-Aktivitäten auf Computern und Mobilgeräten verfolgt.
Systemlog	Automatische Erstellung eines Protokolls von Softwareprozessen.
Testimonial	Konkrete Fürsprache für ein Produkt, eine Dienstleistung, eine Idee oder Institution durch eine Person, die der Zielgruppe meist bekannt ist und mit ihrem Auftritt die Glaubwürdigkeit der Werbebotschaft erhöht.
Tracking-System	System, welches Informationen über den Verlauf der Bewegung und die Lage eines Objektes sammelt.
Workforce Analytics	s. Kapitel 2.2.6.

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AJP/PJA	Aktuelle juristische Praxis/Pratique juridique Actuelle
a.M.	anderer Meinung
ArG	Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel (Arbeitsgesetz, ArG) vom 13. März 1964, SR 822.11
ArGV	Verordnung 3 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3) vom 18. August 1993, SR 822.113
Art.	Artikel
Aufl.	Auflage
BezGer	Bezirksgericht
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) vom 18. April 1999, SR 101
bzw.	beziehungsweise
CHF	Schweizer Franken
Co.	Compagnie
CS	Credit Suisse
DSG	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDV	Elektronische Datenverarbeitung
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, SR 0.101
etc.	et cetera
f.	folgende Seite
ff.	fortfolgende Seiten
FTP	File Transfer Protocol (Dateiübertragungsprotokoll)

GlG	Bundesgesetz über die Gleichstellung von Frau und Mann (GlG) vom 24. März 1995, SR 151.1
GPS	Global Positioning System (Globales Positionsbestimmungssystem)
HR	Human Resources (Personalmanagement)
Hrsg.	Herausgeber
IT	Information Technology (Informationstechnologie)
KMU	Kleine und mittlere Unternehmen
lit.	litera (Buchstabe)
N	Randnote
NCSC	National Cyber Security Centre (Nationales Zentrum für Cybersicherheit)
NZZ	Neue Zürcher Zeitung
OGer	Obergericht
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht OR) vom 30. März 1911, SR 220
PC	Personal Computer (Persönlicher Rechner)
PR	Public Relations (Öffentlichkeitsarbeit)
resp.	respektive
RJN	Le Recueil de jurisprudence neuchâteloise
Rz.	Randziffer
s.	siehe
S.	Seite
SBB	Schweizerische Bundesbahnen
SECO	Staatssekretariat für Wirtschaft
SR	Systematische Rechtssammlung
StGB	Schweizerisches Strafgesetzbuch (StGB) vom 21. Dezember 1937, SR 311.0
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
u.a.	unter anderem
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (URG) vom 9. Oktober 1992, SR 231.1
URL	Uniform Resource Locator (einheitlicher Ressourcenanzeiger)

USA	United States of America (Vereinigte Staaten von Amerika)
UWG	Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986, SR 241
vgl.	vergleiche
z.B.	zum Beispiel
ZBJV	Zeitschrift des bernischen Juristenvereins
ZGB	Schweizerisches Zivilgesetzbuch (ZGB) vom 10. Dezember 1907, SR 210
ZH	Zürich
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften
Ziff.	Ziffer
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZV	Zentralverband Öffentliches Personal Schweiz

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

BAUMGARTNER URS L., Wenn sich der Datenschützer in das Arbeitsrecht einmischt, AJP/PJA, 12/2003, S. 1432 ff.

COSTA GIORDANO, Internet- und E-Mail-Überwachung am Arbeitsplatz, in: Jusletter 9. Januar 2012, www.weblaw.ch (Jusletter/Archiv Suche/Chronologie/2012/Jusletter 9. Januar 2012), besucht am: 15.07.2022.

DÄUBLER WOLFGANG, Angriffe auf den Arbeitnehmer im Internet, in: Müller Roland/Pärli Kurt/Wildhaber Isabelle (Hrsg.), Arbeit und Arbeitsrecht: Festschrift für Thomas Geiser zum 65. Geburtstag, Zürich/St. Gallen 2017, S. 31 ff.

DUNAND JEAN-PHILIPPE, Le harcèlement psychologique (mobbing) en droit privé suisse du travail, RJN 2006, S. 13-45.

EGLI URS, Neue Medien und Arbeitsverhältnisse, ZV-Info Öffentliches Personal Schweiz, Juni 2014, S. 105-109, [zit. EGLI, Neue Medien].

EGLI URS, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter, 17. Januar 2011, www.weblaw.ch (Jusletter/Archiv Suche/Chronologie/2011/Jusletter 17. Januar 2011), besucht am: 15.07.2022, [zit. EGLI, Soziale Netzwerke].

EGLI URS, Wenn die Arbeit Nebensache wird, PersonalSchweiz, Dezember 2012/ Januar 2013, S. 10-12, [zit. EGLI, Arbeit Nebensache].

ETTER BORIS/FACINCANI NICOLAS/SUTTER RETO (Hrsg.), Arbeitsvertrag, Der Einzelarbeitsvertrag (EAV) unter Einbezug der Art. 319-355 OR sowie Art. 361OR/362 OR, Bern 2021 [zit. SHK EAV-BEARBEITER/IN, Art. … N …].

FLAGLIEN ANDERS ORSTEN, Risikoanalyse "Soziale Netzwerke" - Welche Risiken für die Unternehmenswerte birgt die Nutzung sozialer Netzwerke in Unternehmen?, digma, 2/2010, S. 64 ff.

GEISER THOMAS, Darf die Arbeitgeberin den Bewerber googeln?, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter - Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 373 ff, [zit. GEISER, Bewerber googeln?].

GEISER THOMAS, Interne Untersuchungen des Arbeitgebers: Konsequenzen und Schranken, AJP/PJA, 8/2011, S. 1047 ff; [zit. GEISER, Interne Untersuchungen].

GLATTHAAR MATTHIAS, Robot Recruiting, SZW, 1/2020, S. 43 ff.

HOLENSTEIN CHRISTOPH, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, in: Rehbinder Manfred (Hrsg.), Schriften zum Schweizerischen Arbeitsrecht, Heft 53, Bern 2002.

JERMANN ANDREAS, Verwendung von Bildern von Mitarbeitern durch den Arbeitgeber, TREX, 4/2014, S. 230 ff.

LANGHEINRICH MARC/KARJOTH GÜNTER, Soziale Netzwerke als Risiko für Unternehmen, digma, 2/2010, S. 50 ff.

MEIER BETTY-ANNETT, Bewertung des Arbeitgebers im Internet, in: Müller Roland/Geiser Thomas/Pärli Kurt (Hrsg.), RiU – Recht in privaten und öffentlichen Unternehmen, Band/Nr. 24, Zürich/St. Gallen 2018, S. 1-78.

MEIER-GUBSER STEFANIE, Arbeitsrechtlicher Gedankenflug übers UWG, AJP/PJA, 11/2014, S. 1486 ff., [zit. MEIER-GUBSER, Gedankenflug UWG].

MEIER-GUBSER STEFANIE, Haftung des Arbeitnehmers, TREX, 5/2012, S. 292 ff., [zit. MEIER-GUBSER, Haftung].

MEIER-GUBSER STEFANIE, Mobbing, Bossing, schwierige Mitarbeiter und Chefs, TREX, 2/2020, S. 104 ff., [zit. MEIER-GUBSER, Mobbing].

PAIS RAQUEL/AMMANN NOÉMIE, Big Data am Arbeitsplatz, AJP/PJA, 10/2019, S. 1095 ff.

PORTMANN ARMAND, Phishing: Mitarbeiter auf dem Prüfstand, digma, 1/2016, S. 30 ff.

PORTMANN WOLFGANG/RUDOLPH ROGER, Kommentar zum Zehnten Titel des Schweizerischen Obligationenrechts: Der Arbeitsvertrag, Art. 319–362 OR, in: Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Aufl., Basel 2015.

REHBINDER MANFRED/STÖCKLI JEAN-FRITZ, Einleitung und Kommentar zu den Art. 319-330b OR, in: Berner Kommentar zum Schweizerischen Privatrecht, Das Obligationenrecht, Band VI, Die einzelnen Vertragsverhältnisse, 2. Abteilung, Der Arbeitsvertrag, Art. 319-362 OR, 2. Teilband, 2. Aufl., Bern 2010.

ROBERTO VITO/SCHISTER ROMAN, Eingeschränkte Arbeitnehmerhaftung, in: Müller Roland/Pärli Kurt/Wildhaber Isabelle (Hrsg.), Arbeit und Arbeitsrecht: Festschrift für Thomas Geiser zum 65. Geburtstag, Zürich/St. Gallen 2017, S. 381 ff.

RUDIN BEAT, Was darf die Chefin, was die Angestellte? Arbeits- und datenschutzrechtliche Schranken der technischen Überwachung der Internet-Nutzung am Arbeitsplatz, digma, 1/2001, S. 4 ff.

RUDOLPH ROGER, Digitalisierung: Herausforderung an das Arbeitsrecht und die Gerichte, in: Portmann Wolfgang/Heiss Helmut/Isler Peter R./Thouvenin F. (Hrsg.), Gedenkschrift für Claire Huguenin, Zürich/St. Gallen 2020, S. 387 ff.

SCHEIDEGGER HANS-ULRICH/PITTELOUD CHRISTINE, Kommentar zu ArG 6, in: Geiser Thomas/von Kaenel Adrian/Wyler Rémy (Hrsg.), Kommentar zum Arbeitsgesetz, Bundesgesetz vom 13. März 1964 über die Arbeit in Industrie, Gewerbe und Handel, 1. Aufl., Bern 2005.

SCIACCA CHRISTOPHER, Mit 400 000 Stimmen in sozialen Medien, digma, 2/2010, S. 60 ff.

SELMAN SINE/SIMMLER MONIKA, «Shitstorm» – strafrechtliche Dimensionen eines neuen Phänomens, ZStrR, 136/2018, S. 248 ff.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7. Aufl., Zürich/Basel/Genf 2012.

STUTZ MICHÈLE/GEIGER-STEINER ALEXANDRA, Arbeitsrecht/Droit du Travail - Arbeitsrechtliche Fragen rund um Social Media, Anwaltsrevue, 5/2013, S. 212 ff.

STUTZ MICHÈLE/VALLONI NOEMI, Kapitel 5: Social Media im Arbeitsrecht, in: Staffelbach Oliver/Keller Caudia (Hrsg.), Social Media und Recht für Unternehmen, Zürich/Basel/Genf 2015, S. 159 ff.

VON KAENEL ADRIAN/RUDOLPH ROGER, Elektronischer Update-Service zum Praxiskommentar Streiff/von Kaenel/Rudolph, <https://update.schulthess.com/arbeitsvertrag>.

WANTZ SIMONA/LICCI SARA, Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, in: Jusletter 18. Februar 2019, www.weblaw.ch (Jusletter/Archiv Suche/Chronologie/2019/ Jusletter 18. Februar 2019), besucht am: 22.07.2022.

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Internet am Arbeitsplatz, ZBJV 152/2016, S. 307 ff, [zit. WILDHABER/HÄNSENBERGER, Internet].

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Kündigungsfalle Social Media, in: sui-generis 2015, www.sui-generis.ch (sui generis/Archiv Suche/2015) besucht am: 22.07.2022, [zit. WILDHABER/HÄNSENBERGER, Kündigungsfalle].

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Kündigung wegen Nutzung von Social Media – Wenn Arbeit und Privatleben kollidieren, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schinder Benjamin/Wildhaber Isabelle (Hrsg.), Recht im

digitalen Zeitalter - Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 399 ff., [zit. WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung].

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Social Media-Kontakte im Arbeitsverhältnis, in: Müller Roland/Pärli Kurt/Wildhaber Isabelle (Hrsg.), Arbeit und Arbeitsrecht: Festschrift für Thomas Geiser zum 65. Geburtstag, Zürich/St. Gallen 2017, S. 529 ff., [zit. WILDHABER/HÄNSENBERGER, Social-Media-Kontakte].

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Besprechung des Bundesgerichtsentscheids vom 30.06.2017, 8C_79/2016, AJP/PJA 10/2017, S. 1252ff., [zit. WILDHABER/HÄNSENBERGER, Urteil BGer 8C_79/2016].

WILDHABER ISABELLE/KASPER GABRIEL, Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz, in: Müller Roland A./Rudolph Roger/Schnyder Anton K./von Kaenel Adrian/Waas Bernd (Hrsg.), Festschrift für Wolfgang Portmann, Zürich/Basel/Genf 2020, S. 755 ff.

WILDHABER ISABELLE/LOHMANN MELINDA F./KASPER GABRIEL, Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz, ZSR, Band 38 (2019), S. 459 ff.

Urteilsverzeichnis

EGMR, Urteil vom 5. September 2017, Bărbulescu gegen Rumänien, Nr. 61496/08

Urteil des Bundesgerichts, 8C_740/2017 vom 25. Juni 2018

Urteil des Bundesgerichts, 8C_79/2016 vom 30. Juni 2017

Urteil des Bundesgerichts, 8C_448/2012 vom 17. Januar 2013

Urteil des Bundesgerichts, 4A_741/2011 vom 11. April 2012

Urteil des Bundesgerichts, 4A_611/2011 vom 3. Januar 2012

Urteil des Bundesgerichts, 4A_430/2008 vom 24. November 2008

BGE 127 III 310 vom 30. März 2001

OGer ZH, Entscheid vom 20. März 2019, LA180031-O/U

OGer ZH, Entscheid vom 21. August 2018, SB170372-O/U/jv

OGer ZH, Entscheid vom 27. April 2015, SB140436-O/U/eh

OGer ZH, Entscheid vom 27. März 2015, LA150002-O/U

OGer ZH, Entscheid vom 19. September 2012, SB110702-O/U/rc

BezGer ZH, Entscheid vom 29. Mai 2017, GG160246-L

BezGer ZH, Entscheid vom 26. Januar 2016, GG150250-L

Materialienverzeichnis

Bernet ZHAW Studie, Social Media in Organisationen und Unternehmen: Viel Konstanz - auch in Zeiten von Corona, 16. Dezember 2020, abrufbar unter: <https://bernet.ch/studie/bernet-zhaw-studie-social-media-schweiz-2020/> (zuletzt abgerufen am 15. Juli 2022) [zit. Bernet ZHAW Studie].

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Erläuterungen zu Bewertungsplattformen im Internet, Stand März 2009, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/bewertungsplattformen.html> (zuletzt abgerufen am 19. August 2022) [zit. EDÖB, Erläuterungen Bewertungsplattformen].

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Erläuterungen zu sozialen Netzwerken, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html> (zuletzt abgerufen am 19. August 2022) [zit. EDÖB, Erläuterungen soziale Netzwerke].

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich (Bearbeitung durch private Personen), Stand Oktober 2014, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/bearbeitung-von-personendaten-im-privaten-bereich.html> (zuletzt abgerufen am 19. August 2022) [zit. EDÖB, Leitfaden Bearbeitung Personendaten].

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz (für die Privatwirtschaft), Stand September 2013, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/internet--und-e-mail-ueberwachung-am-arbeitsplatz.html> (zuletzt abgerufen am 15. Juli 2022) [zit. EDÖB, Leitfaden Internet- und E-Mailüberwachung].

Nationales Zentrum für Cybersicherheit NCSC, Merkblatt Informationssicherheit für KMUs, Stand 21. Dezember 2020, abrufbar unter: <https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html> (zuletzt abgerufen am 10. September 2022) [zit. NCSC].

Staatssekretariat für Wirtschaft SECO, Mobbing und andere Belästigungen - Schutz der persönlichen Integrität am Arbeitsplatz, Stand 2016, abrufbar unter: <https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Broschuren/mobbing-und-andere-belaestigungen---schutz-der-persoenlichen-int.html> (zuletzt abgerufen am 7. September 2022) [zit. SECO, Mobbing].

Staatssekretariat für Wirtschaft SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz Art. 26, Stand März 2013, abrufbar unter: https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Wegleitungen_zum_Arbeitsgesetz/wegleitung-zu-den-verordnungen-3-und-4-zum-arbeitsgesetz.html (zuletzt abgerufen am 5. August 2022) [zit. SECO, Art. 26 ArGV 3].

1. Einleitung

1.1. Einführung

Abbildung 1: Social-Media-Symbole *Quelle: www.piqsels.com*

Soziale Medien/Social Media sind elektronische Medien, über welche Nutzer und Unternehmen miteinander kommunizieren, mediale Inhalte austauschen oder gemeinsam gestalten. Zu den sozialen Medien zählen Netzwerke wie Instagram, LinkedIn, Facebook, Twitter, Snapchat, XING etc. Aber auch YouTube, Blogs oder Chats wie WhatsApp sind Teil der sozialen Medien. Die Nutzung dieser Plattformen erfolgt sowohl für private wie auch geschäftliche Zwecke. Gemäss Statista (Anbieter für Markt- und Konsumentendaten) gibt es in der Schweiz 2022 insgesamt 7.5 Millionen Nutzer von sozialen Netzwerken. Zum Vergleich: die ständige Wohnbevölkerung in der Schweiz im 2021 wird mit 8.8 Millionen beziffert[1]. Rund etwa zwei Drittel der Nutzer sind täglich in den sozialen Medien aktiv[2].

Die Auswirkungen von sozialen Medien auf die Gesellschaft sind riesig. So finden gerade auch bei den jüngeren Generationen Informationsnutzung und Meinungsbildung nicht mehr in den herkömmlichen Medien, sondern hauptsächlich in den sozialen Medien statt. Dies zeigt, wie stark Denken und Bewusstsein durch die sozialen Medien geprägt werden. Aber auch die Diskussionskultur hat sich durch die Verlagerung der Kommunikation ins Netz stark verändert. Shitstorms, Fake News etc. sind inzwischen Themen, welche die

[1] Bundesamt für Statistik, Stand und Entwicklung Bevölkerung, <https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/stand-entwicklung/bevoelkerung.html>, besucht am: 05.10.2022.
[2] Statista, Statistiken zur Nutzung sozialer Medien in der Schweiz, https://de.statista.com/themen/2782/social-media-in-der-schweiz/, besucht am: 05.10.2022.

Gesellschaft stark beschäftigen und die Schattenseiten der sozialen Plattformen sichtbar machen.

Sowohl Arbeitgeber wie auch Arbeitnehmer sind von diesen Entwicklungen betroffen, was direkten Einfluss auf das Arbeitsverhältnis hat. Einerseits sind da die Unternehmen, welche die vielseitigen Vorteile und das immense Potential von Social Media nutzen wollen. Andererseits gibt es die Mitarbeitenden, welche in der heutigen Zeit einen beachtlichen Teil ihres Soziallebens auf diesen Plattformen abwickeln. Dies hat zur Folge, dass die private und berufliche Nutzung von sozialen Medien zunehmend verschmilzt. Portfolio und Netzwerke von Mitarbeitenden nutzen Arbeitgebende für ihr Employer Branding, neue Mitarbeitende werden über Social Media rekrutiert. Mitarbeitende wiederum kommunizieren von Berufs wegen über die sozialen Medien mit Kunden, knüpfen Kontakte mit Geschäftspartnern, publizieren und werben ihre Arbeitsergebnisse auf den diversen Plattformen etc. Das Potential für Rufschädigungen und Persönlichkeitsverletzungen ist dabei für beide Seiten gross.

Die verschiedenen Nutzungsformen von Social Media bringen zahlreiche arbeitsrechtliche Fragestellungen in den Themenbereichen Datenschutz, Persönlichkeitsschutz, Treuepflicht, Geheimhaltungspflicht etc. mit sich. Aber auch Urheberrechte (Copyrights), Medienrechte und Wettbewerbsrechte sind bei der Nutzung von sozialen Medien im Unternehmenskontext zu berücksichtigen. Diese Masterarbeit widmet sich der Untersuchung der rechtlichen Risiken von sozialen Medien im Rahmen des Arbeitsverhältnisses. Sie erläutert die wichtigsten Themenfelder und rechtlichen Rahmenbedingungen der verschiedenen Problematiken und was diese für Arbeitgeber und Arbeitnehmer bedeuten. Es werden weiters Handlungsmöglichkeiten für die Arbeitgeber aufgezeigt, die im Falle von Missbrauch angewendet, aber auch präventiv umgesetzt werden können.

1.2. Abgrenzung

Die Masterarbeit fokussiert sich auf die Themenfelder und Risiken aus arbeitsrechtlicher Sicht. Die rechtlichen Folgen von Strafrecht, Urheberrecht, Gleichstellungsgesetz, Datenschutzgesetz und Wettbewerbsrecht werden nur am Rande erwähnt. Es ist zu beachten, dass in der Literatur zahlreiche Aufsätze in Zeit- und Festschriften jedoch in der Rechtsprechung spärlich Urteile zum Thema soziale Medien im Arbeitsrecht zu finden sind. Die Arbeit begrenzt sich zudem auf das Arbeitsrecht in der Schweiz sowie private Einzelarbeitsvertragsverhältnisse. Infolge der Zeitvorgabe für die Masterthesis ist die Arbeit

auf die Literaturanalyse beschränkt und verzichtet auf qualitative und quantitative Umfragen.

1.3. Forschungsfragen

Die folgenden drei Forschungsfragen wurden zum Thema formuliert:

Tabelle 1: Masterthesis Forschungsfragen

Hauptfrage	Mit welchen Risiken sind Arbeitgeber bei der Nutzung von sozialen Medien im Arbeitsverhältnis konfrontiert?
Unterfrage 1	Wie gehen Arbeitgeber rechtlich korrekt bei Problemen bei der Nutzung von sozialen Medien durch Arbeitnehmende vor?
Unterfrage 2	Durch welche Massnahmen lassen sich Risiken minimieren?

1.4. Zielsetzung

Die Masterarbeit soll die Thematik der rechtlichen Risiken von sozialen Medien im Arbeitsverhältnis vertieft theoretisch abklären, aber auch Wissen für die Nutzung im berufspraktischen Kontext generieren. Es werden die verschiedenen Spannungsfelder aufgezeigt und die entsprechenden rechtlichen Grundlagen dazu erläutert. Dabei werden die allgemeinen Rechtsgrundlagen zu Datenschutz, Persönlichkeitsschutz, Treuepflicht sowie Geheimhaltungspflicht geprüft. Basierend auf den bekannten Risikofeldern und den wichtigsten rechtlichen Rahmenbedingungen werden Handlungsmöglichkeiten für die Arbeitgeber aufgezeigt. Im Fokus stehen dabei die Überwachungsthematik sowie die diversen Sanktionsmöglichkeiten von der Verwarnung bis zur Kündigung.

Neben der arbeitsrechtlichen Erörterung der Thematik soll in dieser Arbeit auch die HR-Perspektive einfliessen. Dies insbesondere beim Aufzeigen von Möglichkeiten, wie Unternehmen ihre Mitarbeitenden für eine möglichst gefahrenlose Nutzung von sozialen Medien sensibilisieren können.

1.5. Vorgehensweise

1.5.1. Methodisches Vorgehen

Die verschiedenen Problemfelder von sozialen Medien im Arbeitsverhältnis wurden im Rahmen einer Internetrecherche definiert. Es handelt sich dabei nicht um eine

vollständige Aufzählung der verschiedenen Risiken. Der Fokus wurde auf die am häufigsten thematisierten Gefahren gelegt. Für die Risikoanalyse erfolgte eine umfangreiche Gesetzes-, Literatur- und Urteilsanalyse. Diese umfasste u.a. die wichtigsten Kommentare zum Arbeitsvertrag nach Art. 319-362 OR und zum Arbeitsgesetz sowie Materialen von offiziellen Behörden wie bspw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

1.5.2. Struktur

Kapitel 2 dieser Masterthesis befasst sich mit den Risiken thematisch nach Employee-Lifecycle gegliedert. Bei den einzelnen Risikofeldern werden die wichtigsten Fragen zur Thematik, die rechtlichen Grundlagen sowie einzelne Besonderheiten beleuchtet. Mit den arbeitsrechtlichen Instrumenten, welche dem Arbeitgeber zur Verfügung stehen, sowie den Folgen für die Arbeitnehmenden setzt sich Kapitel 3 auseinander. Innerhalb dieses Kapitels wird auch auf die Präventivmassnahmen für Unternehmen eingegangen. Kapitel 4 widmet sich den Erkenntnissen und den daraus folgenden Empfehlungen dieser Masterthesis.

In dieser Masterthesis wird für die Vereinfachung der Lesbarkeit nur die männliche Sprachform verwendet, diese dabei stets geschlechtsneutral verstanden. Diese Form stellt keine Abwertung anderer Geschlechter dar.

2. Die verschiedenen Risiken

Abbildung 2: Übersicht Risiken *Quelle: M. Zai*

2.1. Social-Media-Screening im Bewerbungsverfahren

2.1.1. Ausgangslage

Die Digitalisierung hat sich in den vergangenen Jahren sehr stark auf die Rekrutierung von neuen Mitarbeitenden ausgewirkt. Bewerbungen werden per Mail versendet oder über die Online-Tools der Unternehmen abgewickelt. Die Suche nach neuen Mitarbeitenden findet hauptsächlich im World Wide Web und nicht mehr in den Tageszeitungen statt. So wie Bewerbende die Unternehmen vor dem Versand einer Bewerbung auf deren Webseiten auf Herz und Nieren überprüfen, so ist die Verlockung für die Arbeitgebenden gross, die Namen von Bewerbenden in Suchmaschinen oder sozialen Netzwerken einzugeben, um weitere Informationen über die Kandidaten zu erhalten. Gerade auch beim Active Sourcing in den beruflichen Netzwerken sind ergänzende Auskünfte von den dort dargestellten Kandidaten aus dem World Wide Web verlockend. Hand aufs Herz, welcher Arbeitgeber hat nicht auch schon Google, Bing und Co. bei der Kandidatenauswahl konsultiert? Dabei kollidiert jedoch das Interesse des Arbeitgebers mit dem Recht der Bewerbenden auf Privatsphäre sowie dem Datenschutz.

2.1.2. Anwendbare Rechtsnormen

In Art. 4 DSG sind die allgemeinen Grundsätze zur Datenbearbeitung aufgeführt. So dürfen Personendaten nur rechtmässig erhoben werden und deren Bearbeitung hat nach den Grundsätzen nach Treu und Glauben, Zweckmässigkeit und Verhältnismässigkeit zu erfolgen[3]. Art. 12 DSG geht auf die Persönlichkeitsverletzung ein. So darf die Datenbearbeitung nicht gegen die Grundsätze im DSG verstossen, dürfen ohne Rechtfertigungsgrund Daten einer Person nicht gegen deren ausdrücklichen Willen bearbeitet werden und ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgegeben werden. Keine Persönlichkeitsverletzung liegt vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Die Datenbearbeitung vor Vertragsabschluss wird in Art. 328b OR konkretisiert. Die Datenbearbeitung darf folglich vor Vertragsabschluss für die Abklärung der Eignung für die Arbeitsstelle durchgeführt werden[4]. Das damit verbundene Fragerecht in den

[3] EDÖB, Leitfaden Bearbeitung Personendaten, Ziff. 2.1.1.
[4] STUTZ/VALLONI, Rz. 5.7.

Bewerbungsgespräche umfasst Fragen zur Ausbildung, dem beruflichen Werdegang sowie zu den beruflichen Absichten und Zukunftsperspektiven[5]. Folglich handelt es sich hierbei um Informationen, die einen Arbeitsplatzbezug vorweisen müssen. Nicht erlaubt sind bspw. Fragen zum Gesundheitszustand oder einer Schwangerschaft. Solche Erkundigungen sind nur zulässig, wenn ein Zusammenhang zum Arbeitsverhältnis besteht. Weiters dürfen Fragen zu Religions-, Partei- und Vereinszugehörigkeit nur gestellt werden, wenn der Arbeitgeber eine entsprechende Institution ist. Persönliche Verhältnisse, Eigenschaften und Neigungen, die nicht wesentlich die beruflichen Fähigkeiten mitbestimmen, gehen den Arbeitgeber nichts an und dürfen nicht erfragt werden[6]. Bei Führungs- oder anderen Vertrauenspositionen kann eine Abklärung der Charaktereigenschaften (Führungsverhalten, Verantwortungsbewusstsein, Zuverlässigkeit) sowie dem Freizeitverhalten und den privaten Verhältnissen (Schulden, Vorstrafen) gerechtfertigt sein[7]. Bei der rechtlichen Beurteilung zur Datenerhebung kann unterschieden werden, ob die bewerbende Person die Stelle erhält oder die bewerbende Person abgewiesen wurde[8].

2.1.3. Screening in beruflichen Netzwerken

Auf beruflichen Netzwerken wie XING und LinkedIn stellen sich Personen im beruflichen Kontext dar. Hier sind insbesondere Informationen über Aus- und Weiterbildung, den bisherigen beruflichen Werdegang sowie die geschäftlichen Kontakte zu finden. Die Profile wurden mit der Absicht erstellt, sich karrieremässig darzustellen. Eine Recherche auf solchen Businessnetzwerken ist zulässig, da hier ein ausreichender Arbeitsplatzbezug im Sinne von Art. 328b OR gegeben ist sowie die Zustimmung des Bewerbers angenommen werden kann[9].

Werden in einer Bewerbung Social-Media-Profile vom Kandidaten erwähnt, so stellt dies ein Einverständnis, ja gar eine Aufforderung für HR-Mitarbeitende sowie potenziell vorgesetzten Personen dar, diese Profile zu besuchen[10]. Oftmals sind solche Profile in den Lebensläufen verlinkt. Bei reinen Bewerbungen über ein XING- oder LinkedIn-Profil erübrigt sich die Einverständnisfrage von selbst.

[5] EGLI, Soziale Netzwerke, Rz. 66; STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 5.
[6] EDÖB, Leitfaden Bearbeitung Personendaten, Ziff. 2.2.1.
[7] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 5.
[8] GEISER, Bewerber googeln?, S. 378 ff.
[9] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 9.
[10] STUTZ/VALLONI, Rz. 5.14.

2.1.4. Screening in privaten Netzwerken

Auf Facebook, Instagram und Co. zeigen Personen ihr Privatleben und ihre privaten Interessen. Gleich zu Beginn ist hier die kritische Frage zu stellen, was nützen solche Informationen im Zusammenhang mit dem Arbeitsverhältnis? Freizeitbeschäftigungen und private Interessen in Zusammenhang mit dem beruflichen Kontext einer Person zustellen, hat mehr mit menschlicher Neugierde als mit einem seriösen Auswahlverfahren zu tun. Die Informationen, welche in privaten sozialen Netzwerken gefunden werden, dürften in einem Bewerbungsgespräch nicht erfragt werden[11]. Entsprechend kann der Schluss gezogen werden, dass Screening in privaten Netzwerken nicht gestattet ist[12]. Sowohl die Art der Informationen wie auch deren Präsentation sind primär für den Freundeskreis, allenfalls den erweiterten Bekanntenkreis, gedacht. Folglich sind die Informationen auf diesen Internetseiten privat und werden bei Anwendung der Privatsphäreneinstellung einem bestimmten Personenkreis gezeigt[13]. Werden keine Privatsphäreneinstellungen vorgenommen, sind die Daten öffentlich zugänglich und auch über Suchmaschinen auffindbar. Bei Weitem sind sich nicht alle Nutzer von sozialen Netzwerken über die Datenschutzeinstellungen im Klaren. Folglich kann nicht automatisch davon ausgegangen werden, dass der Kandidat, der sein Profil nicht über Privatsphäreneinstellungen schützt, automatisch einer Datenerhebung durch den potenziellen Arbeitgeber zustimmt[14].

Die Ausnahme bilden auch hier Social-Media-Profile, die in den Bewerbungsunterlagen aufgeführt werden[15]. Ein aktives Anfragen von Seiten Arbeitgeber für den Zugriff auf solche Profile ist jedoch nicht zulässig[16].

2.1.5. Screening über Suchmaschinen

Was auf den Social-Media-Profilen veröffentlicht wird, wird von den Bewerbenden bewusst gesteuert. Die Informationen, welche Suchmaschinen zum eigenen Namen darstellen, sind hingegen von den Bewerbenden nicht kontrollierbar[17]. Hier besteht einerseits eine grosse Verwechslungsgefahr, ob die gefundenen Daten sich auch tatsächlich auf den Max Muster beziehen, dessen Bewerbungsdossier vorliegt oder zu einem ganz anderen

[11] EGLI, Soziale Netzwerke, Rz. 67.
[12] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 10.
[13] STUTZ/VALLONI, Rz. 5.10.
[14] STUTZ/VALLONI, Rz. 5.11.
[15] EGLI, Soziale Netzwerke, Rz. 74; STUTZ/GEIGER-STEINER, S. 213.
[16] EGLI, Soziale Netzwerke, Rz. 73.
[17] EGLI, Soziale Netzwerke, Rz. 79.

Max Muster gehören. Andererseits ist bei Informationen, welche über Suchmaschinen gefunden werden, die Wahrheit der Daten zu hinterfragen[18]. Entsprechend dieser Datenunsicherheit ist eine allgemeine Suchanfrage über Google und Co. abzulehnen[19].
Aber wie heisst es bekannterweise: Wo kein Kläger da kein Richter. Kaum ein Bewerber erfährt, ob er vom potenziellen künftigen Arbeitgeber gegoogelt oder in den Social-Media-Netzwerken gesucht wurde. Somit bleibt eine Zuwiderhandlung der Arbeitgebenden ohne Konsequenzen.

2.1.6. Robot Recruiting

Gemäss der Swiss People Management Analytics Survey[20] verwenden bereits 21 % der Studienteilnehmenden Applikationen zur Kandidatensuche im Internet. Sourcing-Algorithmen durchforschen dabei die beruflichen Netzwerke sowie andere öffentliche Datenbanken, um potenziell passende Personen für das Unternehmen zu finden. Es ist in Anbetracht der fortschreitenden Digitalisierung anzunehmen, dass diese Art der Kandidatensuche zunehmen wird. Entsprechende Umfragen bei HR-Fachleuten in den USA und Deutschland zeigen auf, dass der Einsatz von Algorithmen in der Personalbeschaffung einen festen Platz finden wird[21]. Als Vorteile werden die Effizienzsteigerung im Rekrutierungsprozess und objektivere Einstellungsentscheide gesehen. Für Arbeitgebende, die diese Rekrutierungsart anwenden, gilt zu beachten, dass die Trainingsdaten, mit welchen die selbstlernenden Algorithmen programmiert werden, nicht frei von strukturellen und institutionellen Diskriminierungen sind[22]. Ein Verstoss gegen Art. 3 GlG kann von Bewerbenden kaum nachgewiesen werden. Unternehmen tun sich jedoch selbst einen Gefallen, wenn sie gegenüber der Diskriminierungsthematik sensibilisiert sind und sich darauf verlassen können, dass der Algorithmus für die Kandidatensuche die passendsten Personen, frei von jeglichen Vorurteilen, findet.
Im Zusammenhang mit der neuen europäischen Datenschutzverordnung und dem im 2023 in Kraft tretenden revidierten Schweizer Datenschutzgesetz wird Unternehmen, welche Sourcing-Algorithmen anwenden, geraten, ihre Prozesse genau zu analysieren, ob

[18] GEISER, Bewerber googeln?, S. 383 f.; STUTZ/VALLONI, Rz. 5.16.
[19] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 10.
[20] WILDHABER/KASPER, S. 764 f.
[21] GLATTHAAR, Robot Recruiting, S. 43.
[22] GLATTHAAR, Robot Recruiting, S. 44 f.

diese den neuen Regelungen zu automatisierten Einzelentscheidungen entsprechen [23]. Dabei sind folgende Empfehlungen im Zusammenhang mit Rekrutierungsalgorithmen zu beachten[24]:

- Die Nutzung von Rekrutierungsalgorithmen soll transparent kommuniziert werden (Tatsache des Einsatzes, verfolgter Zweck, Logik des Algorithmus).
- Eine Vollautomatisierung der Prozesse ist zu vermeiden. Diese sind um menschliche Kontrollpunkte zu designen, um so die für automatisierte Einzelentscheidungen erlassenen Sonderregeln zu vermeiden.
- Wo praktikabel, sollen Wahlmöglichkeiten geschaffen werden. Bspw. das Bewerbungen auch ohne vollautomatisierte Beurteilungen möglich sind.

2.1.7. Empfehlungen zu Social-Media-Screening

Ist Social-Media-Screening unter Umständen nicht auch als Pflicht anzusehen[25]? Wer möchte schon einen neuen Mitarbeitenden einstellen, der Verschwörungstheorien im Netz verbreitet oder sich negativ über den bisherigen Arbeitgeber äussert? Es ist jedoch fraglich, wie sehr solche Recherchen nutzen und ob die HR- oder IT-Abteilungen über das entsprechende Know-how verfügen, um diese effektiv durchzuführen. Rechtssicherer und fairer sind die Abklärung im persönlichen Gespräch mit den Kandidaten sowie das Einholen von Referenzauskünften. Zu empfehlen ist, dass die HR-Verantwortlichen die in den Rekrutierungsprozess eingebundenen Personen auf die Dos and Don'ts im Screening aufmerksam machen[26]. LinkedIn und XING-Recherchen sind dabei unproblematisch. Die Finger lässt man besser von allen weiteren Netzwerken und Plattformen. Als Fazit kann gezogen werden, was im persönlichen Bewerbungsgespräch erlaubt ist, kann auch bei der digitalen Recherche angewendet werden[27].

2.2. Nutzung während der Arbeitszeit

2.2.1. Ausgangslage

Eine der wohl häufigsten Problematiken von sozialen Medien am Arbeitsplatz ist deren vermehrt private Verwendung während der Arbeitszeit. WhatsApp Chats beantworten,

[23] GLATTHAAR, Robot Recruiting, S. 45 ff.
[24] GLATTHAAR, Robot Recruiting, S. 52.
[25] EGLI, Neue Medien, S. 109.
[26] STUTZ/GEIGER-STEINER, S. 213.
[27] STUTZ/VALLONI, Rz. 5.8 und 5.9.

den nicht mehr benötigten Plattenspieler auf Facebook zum Verkauf anbieten und eine Instagram Story von der Wanderung vom Wochenende aufbereiten - geht ja alles ganz schnell und kann kurz zwischen der Bearbeitung von Dossier C und Kundentelefonat X erfolgen. Diese Social-Media-Aktivitäten sind vergleichbar mit dem privaten Surfen im Internet: Konzerttickets bei Vorverkaufsstart ordern, die Herbstgarderobe über Zalando aufpeppen und für den Skiurlaub recherchieren. Wo sind hier die Grenzen zu setzen, wenn diese Tätigkeiten während der Arbeitszeit erfolgen? «Kein Problem, ich arbeite schliesslich dafür auch eine Viertelstunde länger, welche ich nicht erfassen werden», sagt sich vielleicht der eine Mitarbeitende. Ein anderer denkt sich: «anstelle des Smalltalks mit den Arbeitskollegen nutze ich diese Zeit lieber für die Pflege meiner Social-Media-Plattformen». Was muss der Arbeitgeber tolerieren und ab wann wird eine Nutzung als exzessiv angesehen? Wie ist der Zugriff während der Arbeitszeit von einem privaten Gerät des Mitarbeiters geregelt? Gibt es diesbezüglich rechtliche Unterschiede im Vergleich zur Nutzung über die Geschäftsgeräte?

2.2.2. Anwendbare Rechtsnormen

Nach Art. 319 OR ist der Arbeitnehmer zur Leistung von Arbeit verpflichtet. Dazu gehört, dass die Arbeitszeit im Interesse des Arbeitgebers und nicht für private Zwecke genutzt wird. Durch die private Nutzung von sozialen Medien kann diese Pflicht verletzt werden. Es liegt auch eine Verletzung der Treuepflicht durch den Arbeitnehmer gemäss Art. 321a OR vor, wenn dieser die Einrichtungen des Betriebs und/oder die Arbeitszeit in übermässiger Weise für private Zwecke beansprucht[28]. Im Rahmen des Weisungsrechts nach Art. 321d OR kann der Arbeitgeber Weisungen zur Infrastruktur oder der Arbeitszeit erlassen.

2.2.3. Recht auf private Nutzung am Arbeitsplatz?

Vielen Arbeitnehmern ist aufgrund der weitverbreiteten Nutzung von Internet und sozialen Medien während der Arbeitszeit nicht bewusst, dass Art und Umfang der Nutzung primär vom Willen des Arbeitgebers abhängig sind. Grundsätzlich stellt der Arbeitgeber das Arbeitsmaterial zur Verfügung und entscheidet aufgrund seines Weisungsrechtes, mit welchen Mitteln die Arbeitnehmer ihre Arbeitspflicht zu erfüllen haben[29]. Arbeitnehmer

[28] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 9; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 404.
[29] EGLI, Soziale Netzwerke, Rz. 34; HOLENSTEIN, S. 51.

können daher nicht verlangen, dass der Arbeitgeber für seine Mitarbeiter einen Internetzugang zur Verfügung stellt[30].

Mittels Vereinbarung oder Weisung kann der Arbeitgeber die private Nutzung von elektronischen Kommunikationsmitteln regeln[31]. Nutzungseinschränkungen können sich insbesondere auf den zeitlichen Rahmen, detailliert auf Zeitdauer und Zeitpunkt, beziehen[32]. Der Vorteil einer klaren zeitlichen Beschränkung ist, dass Arbeitnehmer wissen, in welchem Umfang sich die betriebliche Toleranzgrenze für die Nutzung bewegt[33]. Der EDÖB lehnt eine solche jedoch ab, da die Einhaltung einer solchen Vorgabe kaum kontrollierbar ist[34]. Es liegt weiters im Ermessen des Arbeitgebers zu bestimmen, wie die Arbeitsgeräte genutzt werden dürfen und welche Zugriffe während der Arbeitszeit erlaubt sind[35].

Ein gänzliches Verbot von sozialen Medien während der Arbeitszeit ist umstritten. In Art. 8 EMRK ist das Recht auf Privatleben am Arbeitsplatz verankert. In einem Urteil des EGMR hielt dieses fest, dass Richtlinien eines Arbeitgebers das private soziale Leben am Arbeitsplatz nicht auf null reduzieren dürfen[36]. Ein komplettes Verbot der Nutzung von E-Mail, Telefon und Internet während der Arbeitszeit würde gegen diesen Entscheid verstossen[37]. Eine solche Beschränkung bedarf einem besondere Rechtfertigungsgrund[38]. Ein solcher gilt bspw. bei Gefahr von Leib und Leben bei Verwendung von Mobilegeräten am Steuerstand einer Maschine, im Flugzeug oder in der Intensivstation[39]. Sowohl das Bundesgericht wie auch das EGMR schützen dem Grundsatz nach den Anspruch der Arbeitnehmenden, während der Arbeitszeit private Tätigkeiten erledigen zu können[40].

Andere Rechtsquellen sind der Auffassung, dass es dem Arbeitgeber nicht nur zusteht die Nutzung des Internets und somit auch der sozialen Medien zu reglementieren, sondern diese ganz zu verbieten[41]. Fehlt eine Weisung vom Arbeitgeber, kann davon ausgegangen werden, dass eine Nutzung von sozialen Medien grundsätzlich erlaubt ist, solange die

[30] HOLENSTEIN, S. 51.
[31] HOLENSTEIN, S. 84; REHBINDER/STÖCKLI, Art. 321d OR N 3.
[32] HOLENSTEIN, S. 84 f.
[33] HOLENSTEIN, S. 85.
[34] HOLENSTEIN, S. 85.
[35] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 37.
[36] EGMR, Urteil vom 5. September 2017, Bărbulescu/Rumänien, Nr. 61496/08, E. 80.
[37] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 426.
[38] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 37.
[39] HOLENSTEIN, S. 89.
[40] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 405.
[41] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 17; STUTZ/GEIGER-STEINER, S. 214; STUTZ/VALLONI, Rz. 5.20; Urteil BGer 4A_430/2008 vom 24. November 2008, E. 4.1.

Arbeitsleistung nicht gefährdet und das übliche Mass nicht überschritten wird[42]. So wird geschätzt, dass die private Social-Media-Nutzung im gleichen Ausmass wie das Führen privater Telefongespräche zulässig ist[43]. Hierbei gilt eine Norm von täglich zwei bis drei Telefonaten im Umfang von wenigen Minuten bei einem Vollzeitpensum[44]. Welcher Umfang als exzessive Nutzung angesehen wird, wird unter Kapitel 3.1.5 näher erörtert.

2.2.4. Verwendung von privaten Mobilegeräten

Die Verwendung von privaten Mobilegeräten während der Arbeitspausen und damit auch die Nutzung sozialer Medien über diese, ist zulässig[45]. Eine Verwendung eines privaten Handys während der Arbeitszeit darf nur in besonderen Fällen vollständig untersagt werden[46]. Ausnahmen von der Verwendung privater Geräte können wiederum bei Sicherheitsrisiken vorgeschrieben werden[47]. Da ist ein absolutes Verbot möglich. Liegt kein solcher Fall vor, kann auch während der Arbeitszeit über private Mobiltelefone an sozialen Netzwerken teilgenommen werden, solange dadurch die Arbeitsleistung nach Art. 319 OR nicht beeinträchtigt wird[48]. Somit unterscheidet sich die Nutzung von privaten Mobilegeräten oder Geschäftsgeräten nicht.

2.2.5. Sanktionen bei übermässiger Nutzung

Zu den möglichen Sanktionen bei übermässiger privater Nutzung von Internet und sozialen Medien gehören die schriftliche Abmahnung, Sperrung von Internetzugängen oder Kündigung. Möglich wäre auch, dass der Mitarbeitende den Lohnanspruch für die Zeit, welche er mit der privaten Nutzung des Internets verbracht hat, verliert (s. Kapitel 3.2.2.)[49]. Zur Kündigung herrschen unterschiedliche Meinungen in der Lehre. Einerseits wird die exzessive Nutzung der sozialen Medien im privaten Rahmen während der Arbeitszeit als schwerwiegende Pflichtverletzung des Arbeitsvertrags angesehen, welche den Arbeitgeber ohne vorangegangene Verwarnung zu einer ordentlichen oder gar fristlosen Kündigung des Arbeitsverhältnisses berechtigen kann[50]. Andererseits stützte das

[42] EGLI, Soziale Netzwerke, Rz. 42; PORTMANN/RUDOLPH, Art. 321a OR N 8; STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 17; WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 10.
[43] STUTZ/GEIGER-STEINER, S. 214.
[44] EGLI, Arbeit Nebensache, S. 10.
[45] EGLI, Soziale Netzwerke, Rz. 42.
[46] EGLI, Soziale Netzwerke, Rz. 42.
[47] EGLI, Soziale Netzwerke, Rz. 41.
[48] EGLI, Soziale Netzwerke, Rz. 42.
[49] EGLI, Soziale Netzwerke, Rz. 52.
[50] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 10.

OGer ZH und anschliessend das BGer eine fristlose Entlassung wegen übermässigem Surfen nicht[51]. Hierzu sind zur Beurteilung des Einzelfalls verschiedene Faktoren (s. Kapitel 3.2.3) zu berücksichtigen.

2.2.6. Workforce/People Analytics

Ein weiteres Thema, welches die Thematik der privaten Nutzung von sozialen Medien tangiert, ist Workforce Analytics, auch People Analytics genannt. Mittels Workforce Analytics kann untersucht werden, wie sich die Belegschaft am Arbeitsplatz verhält. Workforce Analytics analysiert und strukturiert mitarbeiterbezogene Daten mittels Software, um personalbezogene Entscheide liefern und die Mitarbeiterplanung optimieren zu können[52]. Mittels technologie-gestützter Analysen kombiniert Workforce Analytics traditionelle Beschäftigungsdaten (z.B. Leistungsbeurteilungen, Krankheitstage oder Saläre) und neue Daten (z.B. Social-Media-Aktivitätsprotokolle, Sensordaten, Verbraucherdaten aus GPS- oder Tracking-Systemen), um Prozesse zur Identifizierung, Einstellung, Bindung und Belohnung von Stellenbewerbenden und Mitarbeitenden zu schaffen[53]. Grundsätzlich muss ein sachlicher Zusammenhang zwischen der Datenerhebung und dem Arbeitsverhältnis bestehen. Das bedeutet, es dürfen nur Daten über den Arbeitnehmer bearbeitet werden, soweit sie deren Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (Art. 328b OR)[54]. Weiters haben Unternehmen die datenschutzrechtlichen Grundsätze der Zweckbindung, Verhältnismässigkeit und Transparenz zu beachten[55]. Laut der Swiss People Management Analytics Survey[56] verwenden 13 % der befragten Unternehmen bereits People Analytics im Compliance-Management zur Analyse von E-Mails und Telefonaten.

2.3. Eigentumsverhältnisse von Accounts und Kontakten

2.3.1. Ausgangslage

Für Unternehmen sind Social-Media-Kontakte wertvoll, da mittels vieler Kontakte die Reichweite bei der Kommunikation und somit die Bekanntheit des Unternehmens und

[51] Urteil BGer 4A_430/2008 vom 24. November 2008, E. 4.3.
[52] PAIS/AMMANN, S. 1095.
[53] WILDHABER/LOHMANN/KASPER, S. 463.
[54] WILDHABER/KASPER, S. 767.
[55] PAIS/AMMANN, S. 1096.
[56] WILDHABER/KASPER, S. 765.

dessen Produkte bzw. Dienstleistungen gesteigert werden kann. Wenn Mitarbeitende, die für das Unternehmen Social-Media-Kanäle mit Inhalten bespielen und Kontakte geknüpft haben, aus der Firma austreten, droht der Verlust von Followern, mitunter sogar an die Konkurrenz. Spätestens jetzt stellt sich die Frage, wem die Accounts gehören und welche Handlungsmöglichkeiten Arbeitgebende haben.

2.3.2. Anwendbare Rechtsnormen

Was der Arbeitnehmer bei der Ausübung seiner vertraglichen Tätigkeit hervorbringt, wird als Arbeitsergebnis bezeichnet. An diesem ist der Arbeitgeber grundsätzlich nach Art. 321b OR (Rechenschafts- und Herausgabepflicht) sowie Art. 339a OR (Rückgabepflicht) berechtigt. Im Rahmen der Rückgabepflicht nach Art. 339a OR haben Arbeitnehmende bei Beendigung des Anstellungsverhältnisses geschäftliche Kontaktdaten dem Arbeitgeber zu übergeben. Während des Arbeitsverhältnisses kann der Arbeitgeber über Art. 321b OR die Herausgabe der Daten verlangen. Die Herausgabe- und Rückgabepflicht beziehen sich ebenfalls auf Daten und Dokumente in elektronischer Form, was das Bundesgericht in einem nicht publizierten Entscheid festhielt[57]. Zu beachten ist, dass sich der Arbeitnehmer keine Kopien dieser Daten und Dokumente aneignen darf[58]. Als Begründung wird dazu die über das Arbeitsverhältnis hinausgehende Geheimhaltungspflicht gemäss OR Art. 321a Abs. 4 genannt. Zwar können Social-Media-Kontakte oder -Inhalte nicht unbedingt als geheim bezeichnet werden, die Herausgabe- und Rückgabepflicht bezweckt jedoch, dass Arbeitnehmende nicht mehr im Besitz der Arbeitsergebnisse sind und diese verwerten können. Dies gilt ebenfalls auch für die Verwendung der Arbeitsergebnisse durch Dritte, wie bspw. durch einen neuen Arbeitgeber. Zu beachten ist, dass diese Thematik in der Schweiz bis anhin nicht gerichtlich behandelt werden musste und eine entsprechende Rechtsprechung fehlt[59].

2.3.3. Eigentumsarten Social-Media-Accounts

Für die verschiedenen Handlungsmöglichkeiten des Arbeitgebers in Bezug auf Accounts sind die Arten von Profilen zu unterscheiden. Hierbei erfolgt folgende Differenzierung[60]:

[57] Urteil BGer 4A_611/2011 vom 3. Januar 2012, E. 4.3.
[58] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 535.
[59] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 530.
[60] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 534.

Tabelle 2: Eigentumsarten Social-Media-Accounts

Privates Social-Media-Profil	Privater Account	Ausschliesslich private Nutzung
	Privater Mischaccount	Privates Profil, welches auch zur geschäftlichen Kontaktpflege genutzt wird
Geschäftliches Social-Media-Profil	Geschäftlicher Account	Ausschliesslich geschäftliche Nutzung
	Geschäftlicher Mischaccount	Geschäftlicher Account, welcher auch zur privaten Kontaktpflege genutzt wird.

2.3.3.1. Privater Account

Bei privaten Accounts müsste der Arbeitnehmer Daten, welche er in Ausübung seiner beruflichen Tätigkeit erlangt hat und welche für den Arbeitgeber relevant sind, diesem zur Verfügung stellen[61]. Eine Durchsetzung ist für den Arbeitgeber jedoch schwierig, da er die Beweislast trägt, jedoch aufgrund des fehlenden Zugriffs auf die Daten die Relevanz kaum nachweisen kann[62]. Das Weisungsrecht des Arbeitgebers reicht nicht aus, um Einsicht in die private Kommunikation des Arbeitnehmers zu nehmen[63].

2.3.3.2. Geschäftlicher Account

Geschäftliche Accounts stellen in der Regel keine Probleme dar, da diese ausschliesslich für geschäftliche Zwecke erstellt und unterhalten werden. Der Mitarbeiter, welcher für einen solchen Account zuständig ist, hat bei Beendigung des Arbeitsverhältnisses diesen zusammen mit den Zugangsdaten herauszugeben[64]. Wird der Account durch den Arbeitgeber weiterbetrieben, was in der Regel der Fall ist, ist zu beachten, dass der Name des ehemaligen Mitarbeiters nicht mehr verwendet werden darf. Ansonsten liegt eine

[61] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 536.
[62] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 536.
[63] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 536.
[64] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 537.

Verletzung der Persönlichkeitsrechte nach Art. 28 ff. ZGB sowie unlauteres Wettbewerbsverhalten nach Art. 2 ff. UWG vor[65].

2.3.3.3. Privater Mischaccount

Diese entstehen in der Regel dann, wenn Arbeitnehmer ihren ursprünglich privaten Account auch für geschäftliche Zwecke nutzen, da sie nicht mehrere Accounts unterhalten möchten. Ein Weisungsrecht des Arbeitgebers für die Nutzung des privaten Accounts zu geschäftlichen Zwecken besteht jedoch nicht[66]. Der Persönlichkeitsschutz der Arbeitnehmenden geht dem Recht des Arbeitgebers am Arbeitsergebnis vor[67]. Begründet wird dies u.a. damit, dass ein solcher Account vom Arbeitnehmer privat betrieben und finanziert wird und davon ausgegangen wird, dass Kontaktbestätigungen der Person des Arbeitnehmers gelten und nicht nur der Person als Vertreter des Arbeitgebers[68]. Der Arbeitnehmer stellt den Account auch nur für die Dauer seiner Anstellung zur Verfügung. Folglich besteht keine Herausgabepflicht der Zugangsdaten jedoch kann eine Übergabe- bzw. Löschungspflicht bezüglich geschäftlicher Kontakte verlangt werden[69].

2.3.3.4. Geschäftlicher Mischaccount

Beim geschäftlichen Mischaccount hat der Arbeitnehmer auf Weisung des Arbeitgebers ein geschäftliches Profil mit seinem eigenen Namen erstellt und pflegt über diesen sowohl geschäftliche wie auch private Kontakte[70]. Es liegt bei der Beendigung des Arbeitsverhältnisses am Arbeitnehmer, belegen zu können, welche Kontakte privat sind und folglich vom Arbeitgeber herausgegeben und auf dem Geschäftsaccount gelöscht werden müssen[71].

2.3.4. Abgrenzung der Account-Arten

Im vorstehenden Kapitel sind die verschiedenen Arten von Accounts festgehalten. In der Praxis ist die Zuteilung jedoch nicht so einfach. Folgende Kriterien können als Hilfestellung für die Klärung der Account-Art dienen[72]:

[65] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 537.
[66] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 538.
[67] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 538.
[68] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 538.
[69] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 538 f.
[70] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 539.
[71] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 540.
[72] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 543.

Tabelle 3: Checkliste zur Feststellung der Eigentumsart von Social-Media-Accounts

Hatte der Arbeitnehmer den Account schon vor dem Stellenantritt errichtet?
Wird der Account hauptsächlich privat oder zu geschäftlichen Zwecken (Inhalte, Netzwerk) genutzt?
Steht dem Arbeitnehmer während der Arbeitszeit Zeit für die Account-Nutzung zur Verfügung?
Wird im Profil der Name des Arbeitgebers verwendet?
Ist eine geschäftliche oder private Mailadresse als Kontaktadresse hinterlegt?
Werden Corporate Design, Logos, Postadresse etc. vom Arbeitgeber verwendet?

2.3.5. Problematik bei der Übertragung von Social-Media-Daten

Arbeitgeber können die Herausgabe von Social-Media-Daten kaum effektiv durchsetzen. Die Problematiken sind vielschichtig. Eine vollständige Kontrolle über die Übergabe der Daten oder auch Löschung ist kaum möglich, da die Daten bei externen Anbietern liegen[73]. Auch können Arbeitnehmende ihre Accounts nur deaktivieren und so eine Löschung vortäuschen.

Um solchen Problemen vorzubeugen, ist mit den Mitarbeitenden zu klären, mit welcher Art von Accounts die Kontakte und Unternehmenskommunikation auf den sozialen Medien erfolgen soll. So herrscht bereits zu Beginn einer Anstellung Klarheit bezüglich Accounts sowohl für Arbeitgeber wie auch Arbeitnehmer. Entsprechende Regelungen könnten auch in einer Social-Media-Richtlinie (s. Kapitel 3.3.1.2) festgehalten werden. Für Mitarbeitende, welche im Rahmen ihres Stellenbeschriebs aktiv auf den sozialen Medien Kontakte und Inhalte pflegen, empfiehlt sich eine individuelle Nutzungsvereinbarung abzuschliessen. In einer solchen könnte bspw. festgehalten werden, dass die Betreuung von geschäftlichen Kontakten nur in einem rein geschäftlich genutzten Profil des Arbeitgebers stattzufinden hat[74].

[73] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 533.
[74] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 548.

2.4. Rufschädigende Postings und Kontakte

2.4.1. Ausgangslage

Die Selbstdarstellung sowie freie Meinungsäusserungen in den sozialen Medien können zu Spannungen zwischen Arbeitnehmer und Arbeitgeber führen. Spätestens mit der COVID 19-Pandemie ist die öffentliche Diskussion von extremen Überzeugungen beinahe zur Normalität geworden. Muss der Arbeitgeber schweigend hinnehmen, wenn sich Mitarbeitende in den sozialen Medien als Verschwörungstheoretiker austoben? Was geht es den Arbeitgeber an, was seine Mitarbeitenden in der Freizeit in den sozialen Medien posten und welche Meinungen sie dabei vertreten? Schwierig wird es insbesondere dann, wenn eine breite Öffentlichkeit von den privaten Posts Kenntnis nimmt, sich das Thema dadurch in den Medien verbreitet und in diesem Zusammenhang auch der Arbeitgeber unter Druck gerät. So das Beispiel des Zürcher Primarlehrers, welcher sich halbnackt auf seinem Instagram-Profil präsentierte[75]. Aber auch private Postings, welche im Zusammenhang mit der beruflichen Tätigkeit erfolgen, können für Arbeitgeber schwierig sein. Ein in den USA verbreitetes Phänomen sind sogenannte Quittoks (Wortkombination aus der Social-Media-Plattform TikTok und to quit, dem englischen Begriff für kündigen). In diesen teilen Mitarbeitende ihre Kündigung öffentlich per Video mit und posten diese auf ihren Social-Media-Kanälen. Oftmals sind diese Botschaften nicht schmeichelhaft für den verlassenen Arbeitgeber[76]. In der Schweiz ist dieser Trend noch nicht angekommen. Hierzulande wird allenfalls mit einem Post bspw. auf LinkedIn über den Stellenwechsel informiert. Solche Mitteilungen sind in der Regel in einem freundlichen Umgangston verfasst, können aber mitunter auch kritisch ausfallen.

Es ist legitim, dass sich Arbeitgebende vor rufschädigenden Postings und Kontakten ihrer Mitarbeitenden schützen möchten. Zu klären ist, wo die Grenzen der Meinungsäusserungsfreiheit im Zusammenhang mit dem Arbeitsverhältnis liegen und ob der Arbeitgeber Vorschriften für die Nutzung von sozialen Medien in der Freizeit erstellen darf.

[75] OBRIST HELENE, Darum sollten Lehrer es besser sein lassen, splitternackt mit Bananen zu posieren, Watson online vom 23. Januar 2019, <https://www.watson.ch/schweiz/kommentar/683908236-warum-lehrer-nicht-nackt-mit-bananen-posieren-sollten>, besucht am: 29.07.2022.

[76] GILLIES CONSTANTIN, Hurra, ich bin weg! Wie man den eigenen Jobwechsel auf Social Media postet., Handelszeitung Online vom 17. Februar 2022, <https://www.handelszeitung.ch/beruf/hurra-ich-bin-weg-wie-man-den-eigenen-jobwechsel-auf-social-media-postet>, besucht am: 10.08.2022.

2.4.2. Anwendbare Rechtsnormen

Art. 16 BV verankert die Meinungsfreiheit in unserer Gesellschaft. Dieses Grundrecht gilt jedoch nicht schrankenlos im Arbeitsverhältnis. Es sind Treuepflichten nach Art. 321a OR zu wahren sowie Weisungen nach Art. 321d OR zu befolgen. Mitarbeitende werden wiederum über Art. 336 Abs. 1 lit. b OR vor Kündigungen im Zusammenhang mit der Ausübung von Verfassungsrechten geschützt.

Was Angestellte in ihrer Freizeit tun, geht den Arbeitgeber grundsätzlich nichts an. Bilder und Äusserungen, welche öffentlich gepostet werden, können aber nicht einfach nur als privat deklariert werden. Dies insbesondere dann, wenn die Handlungen Einfluss auf das Arbeitsverhältnis haben. So kann der Arbeitgeber gegen öffentliche Posts vorgehen, wenn diese der Reputation des Unternehmens, dessen Mitarbeitenden, Kunden und Geschäftspartnern schaden[77]. Die Mitarbeitenden können je nach Schweregrad des Verstosses abgemahnt, entlassen oder auf Schadenersatz verklagt werden (s. Kapitel 3.2)[78]. Auch eine strafrechtliche Klage im Falle von Verleumdung Art. 174 StGB, übler Nachrede Art. 175 StGB oder Beschimpfung Art. 177 StGB ist möglich[79]. Ebenfalls verbietet das UWG in Art. 3 die Herabsetzung/Anschwärzung des Arbeitgebers durch negative Äusserungen[80]. Die folgenden Faktoren sind zu berücksichtigen, wenn es um die Abwägung geht, was mehr zählt «Meinungsäusserungsfreiheit oder Befolgung der Treupflicht?»[81]:

- Inhalt der Äusserung
- Einzelumstände der Äusserung
- Schwere der Beeinträchtigung des Unternehmens durch Äusserung
- Sprachlicher Kontext
- Der zu verantwortende Verbreitungsgrad
- Schutz der persönlichen Verhältnisse und der Ehre anderer Personen

Bei geringfügigen Verstössen, welche durch Unüberlegtheit erklärt werden können, wird eine Verwarnung empfohlen[82]. Bei groben Beleidigungen, die nach Inhalt und Form zu einer erheblichen Ehrverletzung des Betroffenen führen, ist eine ordentliche Kündigung

[77] PORTMANN/RUDOLPH, Art. 321a OR N 5; SHK EAV-ETTER/SOKOLL, Art. 328 OR N 13.
[78] EGLI, Soziale Netzwerke, Rz. 55.
[79] Vgl. Bsp. Klage für Verleumdung: OGer ZH, Entscheid vom 19. September 2012, SB110702-O/U/rc.
[80] MEIER-GUBSER, Gedankenflug UWG, S. 1490 f.
[81] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 406.
[82] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 407.

(s. Kapitel 3.2.3) angezeigt[83]. Wer in Deutschland seinen Vorgesetzten auf sozialen Medien mit Ausdrücken wie Scheisshaufen oder Drecksau beleidigt, muss mit einer fristlosen Kündigung rechnen[84]. Auch in der Schweiz ist bei besonders mutwilligen und schwerwiegenden Verstössen die fristlose Auflösung möglich[85].

Stellt sich heraus, dass die Äusserungen des Arbeitnehmers auf den sozialen Medien sachlich, objektiv und unpolemisch sind, sind diese rechtens. Würde in diesem Fall durch den Arbeitgeber eine Kündigung erfolgen, wäre diese nach Art. 336 Abs. 1 lit. b OR missbräuchlich[86].

Werden vom Arbeitgeber vertraglich Einschränkungen diktiert, welche Arbeitnehmer in seiner persönlichen Freiheit stark begrenzen, sind diese nach Art. 27 Abs. 2 ZGB unzulässig. Eine Richtlinie (s. Kapitel 3.3.1), welche Bestimmungen zum Umgang mit sozialen Medien enthält, sollte dies berücksichtigen und die Einschränkungen nicht zu extrem formulieren.

2.4.3. Rechtsprechung

Das Bundesgericht stützte den Entscheid für die Entlassung eines Polizeibeamten, welcher auf sozialen Medien seine Sympathie für nationalsozialistisches Gedankengut zum Ausdruck gebracht hatte[87]. Die Social-Media-Posts, welche von der Verwaltungskammer nicht als für ein begrenztes Publikum bestimmt angesehen wurden, vermittelten Überzeugungen, die innerhalb der nationalsozialistischen Ideologie entstanden und missbräuchlich, vulgär und der Funktion eines Polizeibeamten unwürdig waren[88].

Gestützt auf das UWG wurde ein ehemaliger Mitarbeiter in der Fracht- und Charter-Schifffahrtsbranche durch das kantonale Gericht Genf verurteilt. Der verurteilte Mitarbeiter hatte nach seiner fristlosen Entlassung auf einer Domain namens Y.com die Domain Y.ch des Arbeitgebers nachgebildet und dabei alte, verrostete und havarierte Schiffe mit dem Logo des Arbeitgebers sowie Bilder der Verwaltungsräte in legerem Tenue und ebensolcher Pose gepostet[89]. Das Bundesgericht stützte das Urteil auf Art. 2 und Art. 3a

[83] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 407.
[84] STUTZ//GEIGER-STEINER, S. 214; VON KAENEL/RUDOLPH, elektronischer Update-Service zum Praxiskommentar, Art. 321a OR N 4.
[85] STUTZ/GEIGER-STEINER, S. 214; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 407.
[86] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 407.
[87] VON KAENEL/RUDOLPH, elektronischer Update-Service zum Praxiskommentar, Art. 321a OR N 7.
[88] Urteil BGer 8C_740/2017 vom 25. Juni 2018, E. 5.1.
[89] VON KAENEL/RUDOLPH, elektronischer Update-Service zum Praxiskommentar, Art. 321a OR N 3.

UWG sowie Art. 49 OR, passte jedoch die Genugtuungszahlung von CHF 25'000.-- auf CHF 10'000.-- an[90].

2.4.4. Posten, Liken, Teilen

Wichtig zu wissen ist auch, dass die Tatbestände der üblen Nachrede sowie der Verleumdung nicht bloss durch einen eigenen Online-Kommentar, sondern schon durch das Weiterverbreiten eines solchen erfüllt werden können[91]. Aber auch das Liken oder Retweeten von Beiträgen ist nicht risikolos[92]. Die Rechtslage hierzu ist noch ein wenig undurchsichtig. So wurde durch das BezGer ZH im 2016 ein Retweet als straflos bezeichnet[93]. Im Jahr 2017 entschied wiederum das BezGer ZH in einem anderen Fall, dass das Liken einer Nachricht Straftatbestand sei[94]. Dieses Urteil wurde jedoch durch das OGer ZH zum Teil aufgehoben[95]. Da ein Liken «lediglich» eine Reaktion auf einen Beitrag ist und ein Retweet ein bewusstes Weiterverbreiten eines Beitrags, würde man meinen, dass letztere Aktion schwerer wiegen würde. Das Liken wird jedoch als Befürwortung einer Ehrverletzung angesehen und nicht als ein blosses Weiterverbreiten[96]. Das Bundesgericht hat sich in einem anderen Zusammenhang zu Retweets geäussert und dies als typische Verbreitungshandlung eingestuft[97].

Es ist ratsam, vor dem Drücken der Like- und Share-Buttons sich nochmals der Konsequenzen dieser Handlung durch den Kopf gehen zu lassen.

2.4.5. Unterscheidung öffentliche und private Äusserungen

Inwieweit die Rechtsprechung Äusserungen auf Social Media wegen ihres privaten Charakters als besonders schützenswert einstuft, ist noch nicht klar[98]. Es ist anzunehmen, dass die Faktoren «Welcher Kommunikationskanal wurde gewählt» und «Vor welchem Publikum erfolgte die Äusserung» bei der Beurteilung einzelner Fälle berücksichtigt werden

[90] Urteil BGer 4A_741/2011 vom 11. April 2012, E. 6.3.
[91] SELMAN/SIMMLER, S. 260.
[92] SELMAN/SIMMLER, S. 261.
[93] BezGer ZH, Entscheid vom 26. Januar 2016, GG150250-L.
[94] BezGer ZH, Entscheid vom 29. Mai 2017, GG160246-L.
[95] OGer ZH, Entscheid vom 21. August 2018, SB170372-O/U/jv.
[96] WALSER RAHEL, Wann ist ein Klick strafbar und wann nicht?, SRF Online vom 30. Mai 2017, <https://www.srf.ch/news/schweiz/wann-ist-ein-klick-strafbar-und-wann-nicht>, besucht am: 02.09.2022; WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 30; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 420 f.
[97] WALSER RAHEL, Wann ist ein Klick strafbar und wann nicht?, SRF Online vom 30. Mai 2017, <https://www.srf.ch/news/schweiz/wann-ist-ein-klick-strafbar-und-wann-nicht>, besucht am: 02.09.2022.
[98] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 15.

müssen[99]. Als öffentlich gilt, was nicht im privaten Rahmen kommuniziert wurde[100]. Doch was wird als privater Rahmen angesehen? Hier ist folgende Definition zu erwähnen: «In einem Posting in der eigenen Chronik oder in einer geschlossenen bzw. geheimen Gruppe, welches für weniger als sechs Freunde zugänglich ist, falls die Freunde zum Erklärenden in einer besonderen persönlichen oder beruflichen Nähebeziehung stehen und der Anlass der Kommunikation privater Natur ist.»[101] Wichtig ist hierbei nicht die Zahl der Adressaten, sondern dass die Empfänger eine persönliche Beziehung (Familien- und Freundeskreis) oder besonderes Vertrauensverhältnis haben[102]. Postings auf Twitter werden als öffentlich angesehen, da es dem Verfasser des Textes nicht mehr möglich ist, die Verbreitung dieser zu kontrollieren[103].

2.4.6. Besonderes Risiko Multiplikatoreneffekt

Durch den Multiplikatoreneffekt können Social-Media-Beiträge sehr schnell eine hohe Reichweite erzielen. Äusserungen und Kommentare können sich rasant, unkontrollierbar und weit verbreiten[104]. Der Schaden, verursacht durch eine digitale Äusserung, ist um einiges höher, als dies eine mündliche Äusserung bewirken könnte. Auch die Möglichkeit, dass bspw. der Arbeitgeber oder Arbeitskollegen Wind von den Äusserungen auf Social-Media-Kanälen bekommen, ist gross. So werden diese spezifischen Umstände der Verbreitungsgeschwindigkeit von Social-Media-Einträgen im Rahmen der Interessenabwägung in der Regel nachteilig für den Arbeitnehmer gewertet[105].

Immer wieder gibt es Fälle, in welchen Angestellte sich als Mitarbeiter ihres Unternehmens auf sozialen Medien präsentieren, dies aber ohne Wissen des Arbeitgebers tun[106]. Ein jüngeres Beispiel dafür, wie schnell Mitarbeitermeinungen viral gehen, ist jenes vom Google-Praktikant aus Zürich[107]. Dieser postete regelmässig auf TikTok Videos über sein Praktikum beim Tech-Riesen und gab diverse Informationen über sein Arbeitsverhältnis

[99] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 15.
[100] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 16.
[101] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 17.
[102] OGer ZH, Entscheid vom 27. April 2015, SB140436-O/U/eh, E. 5.3.1.
[103] HÜRLIMANN BRIGITTE, Schuldspruch gegen "Kristallnacht-Twitterer" bestätigt, NZZ Nr. 97 vom 28. April 2015, S. 12.
[104] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 26.
[105] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 419.
[106] EGLI, Soziale Netzwerke, Rz. 25.
[107] BÜSSER HARRY, TikTok-Video zeigt, Google-Praktikant verdient in Zürich 9000 Franken pro Monat, Handelszeitung Online vom 18. August 2022, <https://www.handelszeitung.ch/unternehmen/tiktok-video-offenbart-google-praktikant-verdient-in-zurich-9000-franken-pro-monat-525610>, besucht am: 19.08.2022.

preis. Seine Videos, in welchen er unter anderem auch über seinen stattlichen Praktikumslohn von CHF 9'000 im Monat berichtete, wurden über eine Million Mal angeschaut. Von einem Journalisten auf die Videos angesprochen, äusserte sich die Pressestelle von Google nicht zu den Löhnen. Das Google jedoch an dieser ungewohnten Lohntransparenz nicht unbedingt Freude hatte, zeigte sich, als manche Videos auf dem Kanal des Praktikanten einige Tage später verschwunden waren. Darunter auch das Video mit den Gehaltsinformationen. Anzumerken ist hier, dass die Treuepflicht des Arbeitnehmers ihm nicht verbietet, mit Dritten über den eigenen Lohn zu sprechen[108]. Ein weiteres Beispiel für die rasante Verbreitung von Social-Media-Postings ist der sogenannte «Kristallnacht-Twitterer». Dieser hatte weniger als 40 Follower, durch Retweets verbreitete sich seine Nachricht jedoch über 40'000 Mal[109].

2.5. Cybermobbing

2.5.1. Ausgangslage

Zu den Schattenseiten der sozialen Medien zählt auch Cybermobbing. Beim systematischen Bedrohen, Beleidigen, Belästigen oder Blossstellen über elektronische Kommunikationsmittel scheint die Hemmschwelle noch tiefer zu sein, als dies durch das physisch persönliche Mobbing der Fall ist. Täter können sich leicht in der Anonymität des Internets verstecken. Oftmals wird von ihnen die mangelnde Medienkompetenz der Opfer ausgenutzt. Ein unsorgfältiger Umgang mit Passwörtern, zu wenig bedachte Konsequenzen beim Posten von Social-Media-Beiträgen oder auch Unwissen bezüglich der Privatsphären-Einstellungen der einzelnen Social-Media-Kanäle werden skrupellos ausgenutzt[110].
Durch die Nutzung von Internet am Arbeitsplatz ist das Risiko für Cybermobbing auch Thema für die Arbeitgeber[111]. Es stellen sich hierzu Fragen wie, inwieweit Arbeitgeber für den Schutz der Mitarbeiter vor Angriffen verantwortlich sind, welche Massnahmen zur Verhinderung von Cybermobbing getroffen werden müssen und ob eine Beistandspflicht besteht, wenn ein Angriff durch Dritte stattfindet.

[108] STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 12.
[109] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 27.
[110] Schweizerische Kriminalprävention, <https://www.skppsc.ch/de/themen/internet/cybermobbing/>, besucht am: 07.09.2022.
[111] EGLI, Soziale Netzwerke, Rz. 57; EGLI, Arbeit Nebensache, S. 11.

2.5.2. Anwendbare Rechtsnormen

Als Mobbing wird ein systematisches, über längere Zeit andauerndes und ohne begründeten Anlass erfolgendes Ausgrenzen eines Gruppenmitglieds durch die eigene Gruppe oder einzelne ihrer Mitglieder bezeichnet[112]. Die Art und Weise, wie sich Mobbing äussern kann, sind vielfältig[113]. Durch die höhere Intensität, den Multiplikatoreneffekt sowie die Lebensdauer der Daten im Internet kann beim Cybermobbing zudem schneller das Vorliegen der für Mobbing erforderlichen Systematik angenommen werden[114].

Aus arbeitsrechtlicher Sicht haben Arbeitgeber für den Schutz der Persönlichkeit und der Gesundheit der Arbeitnehmer zu sorgen. Durch die Fürsorgepflicht gemäss Art. 328 OR sind Arbeitgeber für den Schutz der physischen und psychischen Integrität der Mitarbeitenden verantwortlich[115].

Das ArG konkretisiert unter Art. 6 die Massnahmen, welche zum Gesundheitsschutz notwendig sind[116].

Der betriebliche Charakter von Cybermobbing geht nicht dadurch abhanden, dass es über soziale Netzwerke oder ausserhalb der Arbeitszeiten erfolgt[117]. Es kann der Grundsatz angewendet werden, dass alle Mobbing-Handlungen, die ausserhalb des Internets verboten sind, auch online strafbar sind. Zu den typischen Straftatbeständen von Cybermobbing zählen die Folgenden[118]:

- Art. 143bis StGB Unbefugtes Eindringen in ein Datenverarbeitungssystem
- Art. 144bis Ziff. 1 StGB Datenbeschädigung
- Art. 156 StGB Erpressung
- Art. 173 StGB Üble Nachrede
- Art. 174 StGB Verleumdung
- Art. 177 StGB Beschimpfung
- Art 179^{quater} StGB Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte
- Art. 179^{novies} StGB Unbefugtes Beschaffen von Personendaten

[112] PORTMANN/RUDOLPH, Art. 328 OR N 19; STREIFF/VON KAENEL/RUDOLPH, Art. 328 OR N 17.
[113] SHK EAV-ETTER/SOKOLL, Art. 328 OR N 44.
[114] WILDHABER/HÄNSENBERGER, Internet, S. 320.
[115] PORTMANN/RUDOLPH, Art. 328 OR N 12 und 17.
[116] SCHEIDEGGER/PITTELOUD, Art. 6 ArG N 22.
[117] WILDHABER/HÄNSENBERGER, Internet, S. 320.
[118] Schweizerische Kriminalprävention; <https://www.skppsc.ch/de/themen/internet/cybermobbing/>, besucht am: 07.09.2022.

- Art. 180 StGB Drohung
- Art. 181 StGB Nötigung

2.5.3. Pflichten Arbeitgeber

Nach Art. 2 ArGV 3 haben Arbeitgeber alle Massnahmen zu treffen, die notwendig sind, den Gesundheitsschutz zu wahren, zu verbessern und die physische sowie psychische Gesundheit der Arbeitnehmer zu gewährleisten. Arbeitgeber haben die Mitarbeitenden über die Problematik und Konsequenzen von Cybermobbing aufzuklären[119]. Eine weitere präventive Massnahme ist das Einrichten einer unabhängigen Anlaufstelle mit Schlichtungs-, Beratungs- und Unterstützungsaufgaben[120].

Bei konkreten Verdachtsmomenten zu Cybermobbing-Handlungen ist der Arbeitgeber verpflichtet, den Sachverhalt aufzuklären[121]. Auch im Rahmen von Art. 5 Abs. 3 GlG obliegt dem Arbeitgeber die Pflicht, alle möglichen Vorkehrungen zu treffen, um eine Verbreitung von sexistischen Witzen oder Bildern im betrieblichen EDV-System zu verhindern[122].

2.5.4. Haftung Arbeitgeber

Arbeitgeber, welche Schutzmassnahmen unterlassen, können schadenersatz- und in schweren Fällen genugtuungspflichtig werden[123]. Findet im Zusammenhang mit Mobbing eine Kündigung statt und wird diese nachträglich als missbräuchlich eingestuft, kann dies zu einer Entschädigungspflicht von bis zu sechs Monatslöhnen führen[124].

2.6. Gefährdung der IT-Sicherheit

2.6.1. Ausgangslage

Das Sicherstellen der technischen Sicherheit und der Funktionsfähigkeit der IT-Systeme ist eine anspruchsvolle Aufgabe. Durch die private Nutzung der Systeme durch die Arbeitnehmer erhöht sich das Risiko für Angriffe. Technischer Schaden kann durch Spam, Schadsoftware oder durch die Verwendung von identischen Passwörtern für mehrere

[119] WILDHABER/HÄNSENBERGER, Internet, S. 321.
[120] SECO, Mobbing, S. 31; SHK EAV-ETTER/SOKOLL, Art. 328 OR N 45; WILDHABER/HÄNSENBERGER, Internet, S. 321.
[121] SHK EAV-ETTER/SOKOLL, Art. 328 OR N 46; WILDHABER/HÄNSENBERGER, Internet, S. 321.
[122] BAUMGARTNER, S. 1434.
[123] DUNAND, S. 27 ff.; STREIFF/VON KAENEL/RUDOLPH, Art. 328 OR N 17.
[124] MEIER-GUBSER, Mobbing, S. 106 f.

soziale Netzwerke und Geschäftssysteme entstehen[125]. Im Weiteren stellen Fotos und Informationen von Mitarbeitenden auf der Webseite ein Sicherheitsrisiko für Unternehmen dar. Kriminelle können sich aufgrund dieser Angaben eine falsche virtuelle Identität anlegen und sich mit dieser Zugang zu weiteren schützenswerten Informationen verschaffen[126]. Mittels Phishings kann auch ein Angriff auf das Unternehmens-Netzwerk erfolgen. Der EDÖB führt in seinen Erläuterungen zu sozialen Netzwerken detailliert die weiteren Risiken und Gefahren auf, welche durch eine unvorsichtige Nutzung von diesen Plattformen entstehen[127]. Auch informiert der EDÖB über aktuelle Risiken und Problematiken. So warnte er bspw. im Frühling 2021 über die Datenabflüsse auf LinkedIn. Dabei wurden Benutzer-Identitäten, vollständige Namen, E-Mailadressen, Telefonnummern und Links zu anderen LinkedIn-Profilen gehackt und auf einem spezialisierten Forum zum Verkauf angeboten[128].

2.6.2. Anwendbare Rechtsnormen

Mitarbeitende sind im Rahmen der Sorgfaltspflicht nach Art. 321a OR angehalten, bei der privaten Nutzung von Internet und geschäftlichen E-Mail-Konten, den Arbeitgeber nicht der Gefahr, durch Computerviren geschädigt zu werden, auszusetzen[129]. Sie sind verpflichtet, Sicherheits- und Haftungsrisiken zu vermeiden[130]. Führt ein grobfahrlässiger Verstoss zu einer Infektion des Rechners, wird der fehlbare Arbeitnehmer schadenersatzpflichtig[131]. Für mangelhafte Sicherheitsvorkehrungen trägt jedoch immer der Arbeitgeber die alleinige Verantwortung, da er alle technisch-organisatorischen Massnahmen zur Verminderung des Infektionsrisikos ergreifen muss[132].

2.6.3. Schutz vor Cyberangriffen

Das NCSC empfiehlt Unternehmen verschiedene organisatorische und technische Massnahmen, um das Risiko von Cyberangriffen zu minimieren. U.a. wird die Sensibilisierung der Mitarbeitenden auf die Thematik sowie ein Bedachter Umgang mit

[125] FLAGLIEN, S. 65.
[126] LANGHEINRICH/KARJOTH, S. 50 und 54.
[127] EDÖB, Erläuterungen soziale Netzwerke.
[128] EDÖB, Datenabflüsse bei Sozialen Netzwerken, vom 13. April 2021, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien.html>, besucht am: 08.09.2022.
[129] PORTMANN/RUDOLPH, Art. 321a OR N 8.
[130] WANTZ/LICCI, Rz. 33; WILDHABER/HÄNSENBERGER, Internet, S. 311.
[131] HOLENSTEIN, S. 156.
[132] HOLENSTEIN, S. 156.

Firmeninformationen im Internet empfohlen[133]. Durch Awareness-Aktionen können Mitarbeitende auf das Risiko von Phishing-Angriffen sensibilisiert werden[134].

2.7. Verletzung der Geheimhaltungspflicht

2.7.1. Ausgangslage

Arbeitgeber haben ein grosses Interesse daran, dass Geschäftsdaten mit Geheimnischarakter nicht in falsche Hände gelangen. Aus unüberlegtem Handeln, aber auch durch Böswilligkeit, können Mitarbeitende geheime Informationen über die sozialen Medien verbreiten. Mitarbeitende sind an die Geheimhaltungspflicht gebunden, doch was bedeutet diese in der Praxis? Welche Rechtsnormen schützen Arbeitgeber davor, dass Arbeitnehmer schützenswerte, interne Informationen nicht über soziale Netzwerke austauschen?

2.7.2. Anwendbare Rechtsnormen

Im Rahmen der Sorgfalts- und Treuepflicht nach Art. 321a OR wird in Abs. 4 die sogenannte Geheimhaltungspflicht umschrieben. Erfolgt eine Pflichtverletzung kann der Arbeitgeber auf Unterlassung der Pflichtverletzung sowie bei Verschulden auf Schadenersatz nach Art. 321e OR klagen[135]. Es können auch Disziplinarmassnahmen ergriffen werden. Eine fristlose Kündigung ist jedoch nur bei Unzumutbarkeit der Fortsetzung des Arbeitsverhältnisses, was eine schwere Verletzung der Treuepflicht erfordert, begründet[136]. Die Verweigerung oder Herabsetzung des Lohnes ist bei der Treupflichtverletzung unzulässig, Schadenersatzforderungen können jedoch mit der Lohnforderung verrechnet werden Art. 323b Abs. 3 OR[137]. Auch bei unbedachten Äusserungen, sogenannter Fahrlässigkeit nach Art. 321e Abs. 1 OR, tritt eine zivilrechtliche Haftung ein[138].
Der Verrat von Fabrikations- oder Geschäftsgeheimnissen ist strafbar und kann bei Verletzung nach Art. 162 und 273 StGB auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe gerichtet werden[139].

[133] NCSC, Ziff.3.
[134] PORTMANN, S. 30 ff.
[135] REHBINDER/STÖCKLI, Art. 321a OR N 16.
[136] REHBINDER/STÖCKLI, Art. 321a OR N 16.
[137] PORTMANN/RUDOLPH, Art. 321a OR N 18.
[138] PORTMANN/RUDOLPH, Art. 321a OR N 26.
[139] STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 15.

Stellt der Geheimnisverrat oder dessen Verwertung unlauterer Wettbewerb dar, so hält auch das UWG wirksame Mittel zur Verfügung, so die Einziehung des Gewinns (vgl. dazu Art. 6 und Art. 4 lit. c UWG[140].

2.7.3. Umfang der Geheimhaltungspflicht

Der Geheimnisbegriff ist unter Art. 340 Abs. 2 OR, Art. 162 StGB und Art. 6 UWG geregelt und einheitlich zu verstehen[141]. Ein Geheimnis bezieht sich auf Tatsachen[142],

- die nicht offenkundig und ohne grosse Recherche allgemeinzugänglich sind,
- die nur einem beschränkten Personenkreis bekannt sind,
- deren Weiterverbreitung der Arbeitgeber unterbinden und steuern kann,
- an denen der Arbeitgeber ein berechtigtes Geheimhaltungsinteresse hat und
- für die der Arbeitgeber seinen Geheimhaltungswillen erkennbar gemacht hat.

Alle Informationen, welche allgemein zugänglich sind, dazu zählen u.a. Einträge im Handelsregister, Telefonbuch oder auf der Webseite, gelten nicht als geheimhaltungspflichtig[143]. Auch keine geschützten Geheimnisse sind berufliche Erfahrungen und Branchenkenntnisse, welche der Arbeitnehmer beim Arbeitgeber sammelt[144]. Unter die Geheimhaltungspflicht fallen Fabrikationsgeheimnisse (bspw. Produktionsverfahren und Modelle über Forschungsergebnisse) sowie Geschäftsgeheimnisse aller Art, welche den kaufmännisch-organisatorischen Bereich betreffen (bspw. Kundenverzeichnisse, Preisberechnungen, Personalwesen und Marketingaktionen)[145]. Während des Arbeitsverhältnisses ist die Geheimhaltungspflicht absolut, wohingegen nach Beendigung des Arbeitsverhältnisses eine Lockerung eintritt[146].

2.7.4. Veröffentlichung von Fotos aus dem Arbeitsumfeld

Eine weitere Problematik stellt auch das Posten von Fotos aus dem Arbeitsumfeld dar. Einerseits ist darauf zu achten, wie die Bildrechte geregelt sind (s. Kapitel 2.8.3). Weiters muss sichergestellt sein, dass das gepostete Bild nicht persönlichkeitsverletzend ist.

[140] STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 15.
[141] SHK EAV-MILANI, Art. 321a OR N 38.
[142] SHK EAV-MILANI, Art. 321a OR N 39.
[143] STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 12.
[144] REHBINDER/STÖCKLI, Art. 321a OR N 13; SHK EAV-MILANI, Art. 321a OR N 48–53; STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 12.
[145] REHBINDER/STÖCKLI, Art. 321a OR N 13; SHK EAV-MILANI, Art. 321a OR N 43 f.
[146] MEIER-GUBSER, Gedankenflug UWG, S. 1496; REHBINDER/STÖCKLI, Art. 321a OR N 14; STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 13.

2.8. Nutzung von Mitarbeiterdaten im Rahmen des Employer Brandings

2.8.1. Ausgangslage

Auch Unternehmen kommunizieren mittlerweile offener mit Daten über ihre Mitarbeitenden. Bspw. werden neue Mitarbeitende auf Social-Media-Kanälen begrüsst oder es werden über Mitarbeitenden-Events Berichte gepostet. Weiters werden Namen, Titel, Qualifikationen, Arbeitsgebiete und Erreichbarkeit von Mitarbeitenden zu Werbezwecken sowie für den Kontakt nach Aussen auf verschiedenen Kommunikationskanälen der Unternehmen publiziert[147]. Zwecks Employer Branding werden für die externe Kommunikation oftmals die Mitarbeitenden als Testimonials genutzt. Es fragt sich, wie weit Arbeitgeber Informationen über ihre Mitarbeitenden auf den Social-Media-Kanälen veröffentlichen dürfen und welche Problematiken zu berücksichtigen sind.

2.8.2. Anwendbare Rechtsnormen

In Art. 328b OR ist die Bearbeitung von Personendaten geregelt. Die Verletzung dieses Artikels durch den Arbeitgeber stellt eine Verletzung der Fürsorgepflicht dar. Das Veröffentlichen von Mitarbeiterdaten auf der Unternehmenswebseite oder den sozialen Netzwerken ist dann zulässig, wenn es dem Unternehmenszweck dient. So ist zum Beispiel die Darstellung von Mitarbeitenden mit Kundenkontakt auf öffentlich zugänglichen Plattformen erlaubt. Auch gibt es gesetzlich vorgeschriebene Veröffentlichungen wie der Eintrag im Handelsregister. Die dort publizierten Informationen darf das Unternehmen ebenfalls auf seinen eigenen externen Kommunikationsplattformen verwenden. Eine Einwilligung ist erforderlich, wenn weitere Personaldaten wie Informationen über den bisherigen Werdegang, Ausbildungsabschlüsse, Mitgliedschaften etc. vom Arbeitgeber veröffentlicht werden.

2.8.3. Verwendung von Bildern von Mitarbeitern

Werden Bilder von Mitarbeitenden durch einen externen Fotografen erstellt, ist es wichtig, die Urheberrechte an der Fotografie übertragen zu lassen. Mit der Übergabe beziehungsweise Ablieferung der Bilder erwirbt der Arbeitgeber vorerst nur das sachenrechtliche Eigentum an den vertragsmässig erstellten Fotografien[148]. Nach Art. 6 URG ist Urheberin die natürliche Person, welche das Werk erschaffen hat. Sie kann nach Art. 10

[147] DÄUBLER, S. 1.
[148] JERMANN, S. 230.

URG über die Verwendung des Werks sowie Art. 11 URG über die Bearbeitung des Werks entscheiden. Bei der Beauftragung eines externen Fotografen ist folglich dem Arbeitgeber zu empfehlen, bereits mit der Auftragserteilung in einer schriftlichen Vereinbarung festzuhalten, dass sämtliche Rechte, insbesondere allfällige Urheberrechte, an den zu erstellenden Bildern auf ihn übertragen werden[149]. Nur als Inhaber der umfassenden, ausschliesslichen Nutzungsrechte an den Fotografien seiner Mitarbeiter ist der Arbeitgeber in der Lage, seiner arbeitsrechtlichen Fürsorgepflicht in direkter Weise nachzukommen und unbefugten Bildverwendungen sowohl durch Dritte als auch durch den Fotografen wirksam entgegenzutreten[150].

In dieser Thematik weiters zu beachten ist das Recht am eigenen Bild. Für die Veröffentlichung von Fotos benötigt das Unternehmen gemäss Art. 28 ff. ZGB sowie Art. 12 Abs. 2 lit. b DSG die Einwilligung der Mitarbeitenden. Es handelt sich dabei um eine Unterart des allgemeinen Persönlichkeitsrechts[151]. Dieses erfordert, dass jede Person um Zustimmung erfragt werden muss, sei dies nicht nur für die Erstellung, sondern auch für die Verwendung der Fotografie. Es ist daher Arbeitgebern zu empfehlen, dass sie von den Mitarbeitenden eine schriftliche Einwilligung für die Erstellung und Verwendung (Bspw. Veröffentlichung auf Webseite oder in Drucksachen) der Fotografien einholt[152].

In Art. 3 lit. e DSG ist der Begriff der Datenbearbeitung umschrieben. Hierzu gehören auch das Verwenden und Bekanntgeben von Daten[153]. Das Veröffentlichen der Daten ist in Art. 3 lit. f DSG definiert.

2.9. Social-Media-Aktivitäten als Teil des Arbeitsvertrags

2.9.1. Ausgangslage

Mitarbeitende, die talentiert im Umgang mit sozialen Netzwerken sind und viele Follower haben, sind für Unternehmen wertvoll. In diesem Kapitel geht es darum zu klären, wie weit das Weisungsrecht des Arbeitgebers geht, um die Mitarbeitenden für den Aufbau von Geschäftsbeziehungen sowie die Pflege von Inhalten und Kundenkontakten auf den

[149] JERMANN, S. 231.
[150] JERMANN, S. 231.
[151] JERMANN, S. 231.
[152] JERMANN, S. 231.
[153] PORTMANN/RUDOLPH, Art. 328b OR N 4.

sozialen Medien zu beauftragen oder auch Arbeitgeberbewertungen auf Bewertungsplattformen vorzunehmen.

2.9.2. Rechtsnormen

Dem Weisungsrecht nach Art. 321d OR sind Grenzen gesetzt. Insbesondere müssen Weisungen u.a. einen Zusammenhang mit dem Arbeitsverhältnis haben. So kann folglich keine Anweisung für die Nutzung eines privaten Profils zu geschäftlichen Zwecken erteilt werden. Dies würde zu einer Verletzung der Fürsorgepflicht nach Art. 328 Abs. 1 OR führen, da dies eine unzulässige Verletzung der Privatsphäre des Arbeitnehmers darstellen würde[154].

Die Nutzung eines privaten Social-Media-Accounts für Unternehmenszwecke kann nur aus freiwilliger Bereitschaft durch den Arbeitnehmer erfolgen oder falls diese bei Vertragsabschluss explizit vereinbart wurde. Bspw. bei der Anstellung eines Marketingmitarbeiters wurde bewusst der Entscheid zugunsten einer Person gefällt, welche eine hohe Anzahl an Followern auf Social Media vorweist und so eine höhere Reichweite bei der Unternehmenskommunikation erreichen kann.

Unternehmen können ihre Mitarbeitenden anweisen, Business-Netzwerke zum Aufbau und der Pflege ihrer Geschäftskontakte zu nutzen[155]. Diese Weisung hat sich jedoch auf die Arbeitszeit sowie die geschäftlichen Geräte zu beschränken[156]. Zudem müssen die Mitarbeitenden darauf achten, dass beim Social-Media-Account erkennbar ist, dass sie im Unternehmensauftrag auf dem Netzwerk tätig sind[157]. Dies beugt Risiken im Zusammenhang mit unlauterem Wettbewerb vor, nämlich der eindeutigen Kennzeichnung von Werbung.

2.9.3. Corporate Influencer / Employee Advocacy

Influencer werden für Unternehmen immer wichtiger[158]. Bereits rund zwei Drittel der befragten Organisationen arbeiten mit internen oder externen Meinungsmachern zusammen. Dabei übernehmen die eigenen Mitarbeitenden, die sogenannten Corporate Influencer, die Hälfte des Influencer-Kuchens. Interessant ist, dass insbesondere Verwaltungseinheiten und politische Organisationen auf eigene Mitarbeitende als Influencer

[154] WILDHABER/HÄNSENBERGER, Social-Media-Kontakte, S. 531.
[155] STUTZ/VALLONI, Rz. 5.21.
[156] STUTZ/VALLONI, Rz. 5.22; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 426.
[157] STUTZ/VALLONI, Rz. 5.22.
[158] Bernet ZHAW Studie, S. 5 und 20.

setzen[159]. Corporate Influencer ist ein Arbeitnehmer nicht schon dann, wenn er hin und wieder Inhalte des Unternehmens in sozialen Netzwerken teilt. Von einem Corporate Influencer wird erst gesprochen, wenn der Arbeitnehmer als Content Creator auftritt, also eigene unternehmensbezogene Werbebotschaften entwickelt[160].

Ist ein Corporate Influencer im Rahmen des Arbeitsvertrages tätig, ist auch für diese Tätigkeit das Arbeitsgesetz mit seinen Regelungen zu den Arbeitszeiten Art. 9 ff. ArG sowie Ruhezeiten Art. 15 ff. ArG zu berücksichtigen. Die Abgrenzung, was erfolgt während der Arbeitszeit und was in der Freizeit, kann für Unternehmen zur Herausforderung werden. Influencer sind bekannt dafür, dass sie in reger Interaktion mit ihren Followern stehen und Posts nicht nur während den normalen Arbeitszeiten veröffentlichen und beantworten.

Employee Advocacy ist eine Marketingmethode, bei welcher die Unternehmensmarke durch die eigenen Mitarbeitenden beworben wird. Dabei posten Mitarbeitende Beiträge aus ihrem Arbeitsalltag in den sozialen Netzwerken oder präsentieren ihr Unternehmen positiv bei Referaten oder Branchendiskussionen. Diese Art von Marketing kann weder angeordnet noch gekauft werden. Es lebt von der Glaubwürdigkeit und Authentizität der einzelnen Mitarbeitenden. Der Vorteil dieser Marketingmethode ist, dass diese Empfänger erreicht, bei welchen Botschaften über die üblichen Kommunikations- und Marketingkanäle sonst nicht ankommen. Die Kommunikationsagentur MSL-Group hat hierzu interessante Zahlen erhoben[161]:

- Botschaften, die auf sozialen Netzwerken von Mitarbeitenden verbreitet werden, werden 24-mal häufiger weitergeleitet als solche, die von der Firma selbst stammen.
- Mitarbeiter sind mit zehnmal mehr Personen verbunden als die Firma selbst.

2.10. Arbeitgeberbewertungsportale

2.10.1. Ausgangslage

Dass Bewerbende während eines Auswahlverfahrens möglichst viele Informationen über den potenziell künftigen Arbeitgeber einholen und sich eine entsprechende Meinung

[159] Bernet ZHAW Studie, S. 5 und 20.
[160] HERBERGER MARIE, Arbeitsrechtliche Rahmenbedingungen für Corporate-Influencer, Neue Zeitschrift für Arbeitsrecht, 4/2022, S. 238 ff.; HOFFMANN MICHEL/LEX LAURA, Corporate Influencer & Social Media Guidelines, Recht Digital (RDi), 5/2021, S. 242 ff.
[161] STAMM EUGEN, Alle arbeiten jetzt im Marketing, NZZ vom 15. August 2017, S. 25.

bilden, ist nur legitim. Nebst den von Unternehmen auf der eigenen Webseite veröffentlichten Informationen, werden oftmals auch Arbeitgeberbewertungsseiten konsultiert. Auf diesen sind individuelle Feedbacks sowie Bewertungen zu diversen Kriterien von ehemaligen und aktuellen Mitarbeitenden ersichtlich. Zu den bekanntesten Arbeitgeberbewertungsportalen zählen Kununu, Glassdoor und Indeed. Aber auch auf Stellenseiten wie jobs.ch können Bewertungen über den Arbeitgeber hinterlegt werden. Die veröffentlichten Bewertungen erscheinen nicht nur auf den entsprechenden Bewertungsportalen, sondern es zeigt ebenfalls eine Zusammenfassung an, wenn eine Jobsuche über Google gestartet wird.

Gemäss einer deutschen Umfrage konsultieren rund 50 % der Stellensuchenden Arbeitgeberbewertungsseiten[162]. Ob eigene Bewertungen geschrieben wurden, untersuchte eine Schweizer Studie und wurde von rund 13 % der Teilnehmenden bejaht[163]. Bei vorwiegend positiven Kommentaren sind die Bewertungsportale für die Unternehmen eine erfreuliche zusätzliche Werbeplattform. Häufen sich jedoch negative Bewertungen, kann dies den Ruf eines Unternehmens und folglich die Arbeitgebermarke schädigen. Unternehmen stehen vor der Frage, wie aktiv sie sich auf diesen Plattformen bewegen und wie sie auf Kommentare reagieren sollen. Welche Reaktionsmöglichkeiten stehen bei negativen (ungerechtfertigten) Kommentaren zur Auswahl? Aber auch Mitarbeitende haben sich an Spielregeln zu halten, wenn sie Bewertungen abgeben.

2.10.2. Anwendbare Rechtsnormen

Gleich mehrere Rechtsgebiete sind in die Thematik der Bewertungsplattformen involviert. Nebst dem Arbeitsrecht sind das Gesetz über den unlauteren Wettbewerb, das Datenschutzgesetz sowie das Strafgesetz betroffen. Das Wettbewerbsrecht ist dann tangiert, wenn durch die getätigten Äusserungen auf den Bewertungsplattformen Herabsetzung nach Art. 3 Abs. 1 lit. a UWG oder Irreführung nach Art. 3 Abs. 1 lit. b UWG erfolgt. Nebst diesen beiden Tatbeständen sind noch zahlreiche weitere unter diesem Artikel im UWG zu finden.

[162] Business Insider, Wie Arbeitgeberbewertungen im Netz die Job-Wahl beeinflussen, Business Insider Online vom 19. April 2021, <https://www.businessinsider.de/karriere/bewerbung/wie-arbeitgeberbewertungen-im-netz-die-job-wahl-beeinflussen/>, besucht am: 12.08.2022.
[163] MEIER B.-A., S. 65.

Das Strafrecht ist bezüglich Bewertungsplattformen hauptsächlich mit Ehrverletzungsdelikten tangiert. Üble Nachrede, Verleumdungen, Beschimpfungen sowie der Verrat von Geschäfts- und Fabrikationsgeheimnissen sind in den Art. 173-179 StGB geregelt.

2.10.3. Was Bewerter beachten müssen

Mitarbeitende unterliegen während des Arbeitsverhältnisses der Treuepflicht nach Art. 321a Abs. 1 OR. Diese Pflicht verlangt, dass keine dem Arbeitgeber wirtschaftlich schädigenden Aktivitäten vorgenommen werden dürfen[164]. Negative Äusserungen resp. Bewertungen im Internet können diese Pflicht verletzen[165]. Wie umfangreich die Treuepflicht ist, hängt vom konkreten Arbeitsverhältnis, genauer genommen von den betrieblichen Umständen sowie den Aufgaben und der Stellung des Arbeitnehmers ab (Art. 321e OR)[166]. So wird von Kadermitarbeitenden eine umfangreichere Treuepflicht verlangt als von normalen Angestellten[167]. Der Treuepflicht entgegengesetzt steht die freie Meinungsäusserung, welche in Art. 16 BV verankert ist[168]. Bei der freien Meinungsäusserung wird grundsätzlich zwischen Tatsachenbehauptungen und Werturteilen unterschieden[169]. Tatsachenbehauptungen müssen der Wahrheit entsprechen und beweisbar sein, Werturteile dürfen nicht unnötig herabsetzend oder beleidigend sein[170].

Ab wann ist eine Meinung nicht nur mehr als kritisch, sondern als schädigend anzusehen? Ein Faktor ist hierbei, ob die Äusserung in einem kleinen privaten Kreis oder öffentlich abgegeben wurde[171]. Wichtig ist auch, dass die Kritik objektiv und unpolemisch geäussert wird[172]. Weiters zu beachten ist, dass die Kommentare weder Ehrverletzungen, persönliche Namen, noch Geschäfts-, Fabrikations- oder Berufsgeheimnisse enthalten.[173]

Von den Arbeitnehmern kann aus der Treuepflicht nach Art. 321a OR auch keine positive Bewertung erzwungen werden.

Gibt es rechtliche Unterschiede, ob Arbeitgeberbewertungen als aktiver oder ehemaliger Mitarbeiter vorgenommen werden? Die rechtliche Situation ändert sich tatsächlich leicht.

---

[164] REHBINDER/STÖCKLI, Art. 321a OR N 3.
[165] STUTZ/VALLONI, Rz. 5.28.
[166] MEIER B.-A., S. 27; STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 2.
[167] PORTMANN/RUDOLPH, Art. 321a OR N 10 und 14; STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 2.
[168] STUTZ/VALLONI, Rz. 5.28.
[169] EDÖB, Erläuterungen Bewertungsplattformen.
[170] EDÖB, Erläuterungen Bewertungsplattformen.
[171] MEIER B.-A., S. 29; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 407 f.; vgl. OGer ZH, Entscheid vom 27. März 2015, LA150002-O/U, E. 2.2.
[172] OGer ZH, Entscheid vom 27. März 2015, LA150002-O/U, E. 2.2.
[173] MEIER B.-A., S. 75.

Mit Beendigung des Arbeitsverhältnisses endet grundsätzlich auch die Treuepflicht[174]. Bestehen bleibt hingegen in einem gelockerten Rahmen die Geheimhaltungspflicht[175].

2.10.4. Was Unternehmen beachten müssen

Wenn Unternehmen Profile auf den Arbeitgeberbewertungsportalen aktiv mittels eines Accounts pflegen, besteht ein Vertrag mit der Plattformbetreiberin. In diesem Falle haben Arbeitgeber die Möglichkeit, Bilder, Videos und Werbetexte auf der Plattform zu schalten. Profile können aber auch ohne aktives Mitwirken der Unternehmen entstehen. Dies ist dann der Fall, wenn ehemalige oder aktive Mitarbeitende eine Bewertung über den Arbeitgeber schreiben. Hierbei besteht zwischen dem Unternehmen und der Bewertungsplattform kein Vertrag.

Ob ein Vertrag zwischen der Betreiberin der Bewertungsplattform und dem bewerteten Unternehmen besteht, ist dann wichtig, wenn das Unternehmen gegen negative Kommentare vorgehen möchte. Ohne Vertragsverhältnis besteht keine Möglichkeit, die schlechten Bewertungen loszuwerden oder auf dem Portal eine Stellungnahme zu publizieren.

In der Regel beinhalten die AGB der Bewertungsplattformen, dass Kommentare mit beleidigenden, verleumderischen, sittenwidrigen, rassistischen oder ähnlichen Inhalten nicht erlaubt sind. Wenn sie nicht durch die Plattformen selbst erkannt und beseitigt wurden, können Unternehmen deren Löschung verlangen.

2.10.5. Handlungsmöglichkeiten für Unternehmen

Unternehmen haben die Möglichkeit, sowohl arbeitsrechtlich als auch straf- und zivilrechtlich gegen schädigende Bewertungen vorzugehen. Soweit die Theorie, welche in der Praxis aus unterschiedlichen Gründen selten angewendet wird.

Dass Unternehmen gegen Bewertungsplattformen rechtlich vorgehen, ist gemäss einer qualitativen Untersuchung kaum wahrscheinlich[176]. Unternehmen beschränken sich bisher hauptsächlich auf Stellungnahmen auf den Plattformen. Es ist ratsam, dass Unternehmen regelmässig die Plattformen auf neue Kommentare durchsuchen und bei kritischen Bewertungen allenfalls Stellungnahmen abgeben. Diese sollten unbedingt auf sachlicher Ebene erfolgen. Kommentare auf Bewertungsportalen können durchaus auf Ver-

[174] PORTMANN/RUDOLPH, Art. 321a OR N 2; STREIFF/VON KAENEL/RUDOLPH, Art. 321a OR N 2.
[175] PORTMANN/RUDOLPH, Art. 321a OR N 27; STREIFF/VON KAENEL/RUDOLPH, Art. 321a, OR N 13.
[176] MEIER B.-A., S. 72.

besserungspotential hinweisen und sollten daher von den Unternehmen auch selbstkritisch betrachtet werden.

Dem Unternehmen stehen verschiedene Massnahmen gegen die Treuepflichtverletzung durch Mitarbeitende zur Auswahl. Es kann gerichtlich eine Unterlassung der Pflichtverletzung sowie Schadenersatz nach Art. 321e Abs. 1 OR eingeklagt werden[177]. Hierbei ist zu beachten, dass die Beweislast der Treuepflichtverletzung grundsätzlich beim Arbeitgeber liegt[178]. Die Problematik dabei ist, dass die Kommentare auf den Plattformen anonym abgegeben werden und Arbeitgeber kaum beweisbare Rückschlüsse haben, von wem die Bewertung verfasst wurde.

3. Arbeitsrechtliche Instrumente

3.1. Überwachungsmöglichkeiten

3.1.1. Ausgangslage

Das Überwachen von Mitarbeitenden ist eine Interessensabwägung zwischen dem betrieblichen Interesse sowie der Einhaltung des Persönlichkeitsschutzes der Arbeitnehmenden[179]. Die Gefahr besteht, dass durch eine Überwachung das Betriebsklima leiden kann. Wer fühlt sich schon wohl, wenn er weiss, dass er permanent unter Kontrolle steht und jeder Schritt, jedes Wort oder jede Handlung am PC aufgezeichnet wird? Schlechte Stimmung bis hin zu gesundheitlichen Beeinträchtigungen können durch Überwachungsanlagen bei betroffenen Mitarbeitenden ausgelöst werden[180]. Das Ausspionieren von Mitarbeitenden auf Social Media macht auch in den USA Schlagzeilen. So wurde Tesla mit dem Vorwurf konfrontiert, über eine PR-Firma seine Mitarbeitende auf Facebook überwacht zu haben, um so u.a. an Informationen über eine mögliche Gewerkschaftsgründung zu gelangen[181]. Solche Schlagzeilen können für Unternehmen rufschädigend sein und ein negatives Image in der Öffentlichkeit hinterlassen. Für zukünftige Bewerbende wirkt es

[177] REHBINDER/STÖCKLI, Art. 321a OR N 16.
[178] STREIFF/VON KAENEL/RUDOLPH, Art. 321e OR N 13.
[179] SECO, Art. 26 ArGV 3, Ziff. 3.1.
[180] SECO, Art. 26 ArGV 3, Ziff. 1.
[181] Finanzen.net, Tesla-Aktie: Tesla soll Mitarbeiter über Social Media überwacht haben, finanzen.net Online vom 18. Juni 2022, <https://www.finanzen.net/nachricht/aktien/in-der-kritik-tesla-aktie-tesla-soll-mitarbeiter-ueber-social-media-ueberwacht-haben-11441013>, besucht am 12.09.2022.

mitunter abschreckend, sich bei einem Unternehmen zu bewerben, welches in der Öffentlichkeit für Überwachungsmassnahmen bekannt ist.
Wichtig ist es für Arbeitgebende zu wissen, dass die Ahndung von betriebsinternen Straftaten Sache der Polizei ist[182]. Es ist nicht die Aufgabe des Unternehmens, sich diese Rolle anzueignen. Denn rechtlich sind dem Arbeitgeber bei der Sammlung von Beweisen Grenzen gesetzt. Werden diese überschritten, bekommt er umgehend die Quittung. Vom Arbeitgeber nicht berechtigt erhobene Überwachungsdaten sind in einem Strafverfahren nicht verwendbar[183].

3.1.2. Rechtsnormen zur Datenbearbeitung

Eine Vielzahl von Rechtsbestimmungen regeln die Thematik der Datenbearbeitung im Arbeitsrecht. Im Rahmen von Art. 12 Abs. 1 DSG wird vorgeschrieben, dass beim Bearbeiten von Personendaten die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden darf[184]. Die Verletzung der Persönlichkeit erfolgt dann widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, nicht durch ein überwiegendes privates oder öffentliches Interesse oder durch das Gesetz gerechtfertigt ist, so Art. 13 Abs. 1 DSG. Die Datenbearbeitung hat zudem laut Art. 4 DSG nach den Prinzipien der Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung und Transparenz zu erfolgen[185]. Ein schutzwürdiges Bedürfnis zur Kontrolle, welche Webseiten am Arbeitsplatz aus privaten Gründen konsultiert werden, hat der Arbeitgeber nicht[186]. Art. 8 DSG hält fest, dass jede Person vom Inhaber von Datensammlungen Auskunft darüber verlangen kann, ob Daten über sie bearbeitet werden. Der Arbeitgeber muss demnach der angestellten und um diese Information nachfragenden Person Auskunft erteilen über[187]:

- Alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten.
- Den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

[182] SECO, Art. 26 ArGV 3, Ziff. 1.
[183] SECO, Art. 26 ArGV 3, Ziff. 1.
[184] BAUMGARTNER, S. 1433.
[185] STUTZ/VALLONI, Rz. 5.45.
[186] GEISER, Interne Untersuchungen, S. 1056.
[187] EDÖB, Leitfaden Internet- und E-Mailüberwachung, Ziff. 8.1.

Die Datenbearbeitung durch den Arbeitgeber wird in Art. 328b OR geregelt. Diese ist nur dann erlaubt, soweit sie die Eignung der Arbeitnehmer für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich ist[188].

3.1.3. Rechtsnormen zu Überwachungs- und Kontrollsystemen

Art. 26 Abs. 1 ArGV 3 verbietet den Einsatz von Überwachungs- und Kontrollsystemen zur generellen Verhaltensüberwachung am Arbeitsplatz[189]. Für das Nutzen von sozialen Medien am Arbeitsplatz bedeutet dies, dass eine ständige personenbezogene Auswertung von Logdaten für die Überwachung des Nutzungsverhaltens nicht zulässig ist[190]. U.a. dürfen Informatikmittel wie Spyware, Systemlogs etc., welche eine Aktivitätenüberwachung am Computer ermöglichen, die Überwachung mittels Computersysteme und -netzwerken sowie die Überwachung von Internet (URL, E-Mail, FTP) zur Verhaltensüberwachung nicht eingesetzt werden[191].

Das Überwachungsverbot gilt jedoch nicht als absolut, denn Art. 26 Abs. 2 ArGV 3 lässt eine Überwachung und Kontrolle aus anderen wichtigen Gründen zu. So bilden gewisse Branchen in der Privatwirtschaft wie Banken, welche erhöhte Compliance-Anforderungen zur Verhinderung von Insiderhandel, Korruption etc. erfüllen müssen und hierzu eine systematische Überwachung und Auswertung von Daten vornehmen müssen, eine Ausnahme[192]. Das ArG setzt für eine Überwachung voraus, dass das Betriebsinteresse überwiegen muss sowie die Verhältnismässigkeit einzuhalten ist[193]. Als Betriebsinteresse gilt u.a. die Sicherheit der Arbeitnehmenden und von Dritten zu wahren. Bei der Verhältnismässigkeit ist zu beachten, dass Überwachungs- und Kontrollsysteme so gestaltet und eingesetzt werden, dass eine Gefährdung der Persönlichkeit der Arbeitnehmenden in höchstmöglichem Mass begrenzt wird[194]. Mitarbeitende sind darüber zu informieren, in welcher Form eine Überwachung stattfindet[195]. Ihnen ist transparent aufzuzeigen, welche Nutzungsregeln sie im Bereich der Informatik befolgen müssen und in welchen Bereichen Überwachungs- und Kontrollsysteme eingesetzt werden dürfen[196]. Dazu gehören auch die

[188] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18.
[189] RUDIN, S. 5.
[190] EDÖB, Leitfaden Internet- und E-Mailüberwachung, Ziff. 4.
[191] SECO, Art. 26 ArGV 3, Ziff. 2.
[192] STUTZ/VALLONI, Rz. 5.45.
[193] SECO, Art. 26 ArGV 3, Ziff. 3.1 und 3.2.
[194] SECO, Art. 26 ArGV 3, Ziff. 3.2.
[195] SECO, Art. 26 ArGV 3, Ziff. 3.2.
[196] SECO, Art. 26 ArGV 3, Ziff. 3.3.

Aufklärung über die internen Regeln zur Nutzung von Internet und E-Mail-Account sowie Verhaltensmassnahmen des Arbeitgebers bei Zugriff auf den E-Mail-Account infolge Abwesenheit der Arbeitnehmenden (Krankheit, Ferien etc.)[197].

3.1.4. Auswertungsformen

Der Leitfaden des EDÖB zur Internet- und E-Mail-Überwachung am Arbeitsplatz dient einerseits der Sensibilisierung, andererseits ist es eine Auslegungshilfe, insbesondere für Art. 26 ArGV 3 und generell für die rechtlichen Bestimmungen zum Persönlichkeitsschutz[198]. Gemäss dem Leitfaden darf keine personenbezogene Auswertung der Logfiles zur Feststellung eines Internet- oder E-Mail-Missbrauchs am Arbeitsplatz erfolgen[199]. Erst nach einem festgestellten Sachverhalt darf dies zur Identifikation des fehlbaren Arbeitnehmers vorgenommen werden. Der EDÖB unterscheidet zwischen drei Auswertungsformen von Randdaten (s. Tabelle 4: Auswertungsformen von Randdaten). Dabei verweist er auf das Prinzip der Verhältnismässigkeit. Der Arbeitgeber muss dabei immer diejenige Form der Auswertung wählen, welche für den angestrebten Zweck (Verhinderung/Aufdecken von Missbräuchen) geeignet ist und den schwächsten Eingriff in die Persönlichkeitsrechte der angestellten Person darstellt[200].

Nicht eindeutig kann die Frage beantwortet werden, wie die Information bezüglich der Überwachung zu erfolgen hat. Ob alleine der Erlass eines Nutzungsreglements, in welchem auf die Möglichkeit der Überwachung hingewiesen wird, genügt oder ob die Mitarbeitenden nach Entstehung des Verdachts nochmals konkret gewarnt werden müssen, wird unterschiedlich interpretiert[201]. Wurde ein Nutzungsreglement für alle Mitarbeitenden transparent kommuniziert, sollte dies eigentlich genügen. Mit einer expliziten Information über die Überwachung nach Aufkommen eines schweren Verdachts, wird der fehlbare Mitarbeiter wohl sein Verhalten ändern und könnte infolge fehlender Beweise nicht überführt werden. Arbeitgeber hätten auf diese Weise kaum Möglichkeiten, brauchbare Beweise zu sammeln und somit fehlbare Mitarbeitende zu sanktionieren, was gerade

[197] SECO, Art. 26 ArGV 3, Ziff. 3.3.
[198] COSTA, Rz. 7.
[199] COSTA, Rz. 4.
[200] EDÖB, Leitfaden Internet- und E-Mailüberwachung, Ziff. 7.
[201] WANTZ/LICCI, Rz. 34; a. M. HOLENSTEIN, S. 120; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 424.

bei einem schwerwiegenden Verdacht zu einer erheblichen Belastung der künftigen Zusammenarbeit führen würde.

Tabelle 4: Auswertungsformen von Randdaten[202]

Anonyme Auswertung (nicht-personenbezogen)	
Randdatenfiles sind immer personenbezogen (Bspw. E-Mailadresse, IP-Adresse oder Kennnummer). Eine anonyme Auswertung dieser Randdaten bedeutet nicht, dass sie anonymisiert werden müssen, sondern die Ergebnisse der Auswertung müssen in rein statistischer Form, also ohne Personenbezug, dargestellt werden. Die Erhebung kann zeitlich und sachlich unbeschränkt erfolgen[203].	Beispiel einer anonymen Auswertung: Wie viele Internetseiten mit pornografischem Inhalt werden durch die Belegschaft pro Monat angesurft?
Pseudonyme Auswertung (Personenbezogen, nicht-namentlich)	
Rohdaten (Logfiles) weisen einen direkten Bezug zu Personen auf. Im Resultat der Auswertung muss der direkte Personenbezug durch die Vergabe von Pseudonymen verhindert werden.	Beispiel einer pseudonymen Auswertung: Gibt es in einer bestimmten Abteilung Mitarbeitende, welche pro Woche mehr als 100 Mails versenden? Die Mitarbeitenden, welche dieses Kriterium erfüllen, werden mit Pseudonymen versehen aufgelistet.
Personenbezogene Auswertung (Namentlich)	
Das Resultat der Randdaten wird konkretisiert auf eine oder mehrere Personen dargestellt. Eine solche Auswertung darf nur durchgeführt werden, wenn mind. ein **konkreter Missbrauchsverdacht** besteht. Eine solche Erhebung ist stichprobenweise, während einer gewissen Zeit möglich[204].	Welche Mitarbeitende surfen pro Tag mehr als zwei Stunden?

Die Voraussetzungen zur Überwachung der Mitarbeitenden sind auch abhängig davon, wie die Nutzung von sozialen Medien in den internen Richtlinien geregelt ist. Es werden in den nachfolgenden beiden Unterkapiteln folgende Voraussetzungen unterschieden:

[202] EDÖB, Leitfaden Internet- und E-Mailüberwachung, Ziff. 7.
[203] WANTZ/LICCI, Rz. 34.
[204] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 424.

3.1.4.1. Nutzung von sozialen Medien ist verboten oder beschränkt

Der Arbeitgeber hat in diesem Fall das Recht, die Einhaltung seiner Weisung zu kontrollieren[205]. Dabei sind die datenschutz- und arbeitsrechtlichen Vorgaben zu berücksichtigen. Die Belegschaft ist vorgängig über die Überwachung zu informieren. Eine totale Überwachung aller Social-Media-Aktivitäten der Mitarbeitenden mittels einer Spyware ist jedoch nicht zulässig[206].

3.1.4.2. Nutzung von sozialen Medien ist erlaubt oder nicht geregelt

Sofern den Mitarbeitenden die Nutzung von Internet am Arbeitsplatz für private Zwecke erlaubt wurde oder nicht geregelt ist, sind die Grenzen für die erlaubte Nutzung erheblich weiter ausgelegt und die Kontrollrechte des Arbeitgebers gehen weniger weit[207]. In diesen Fällen ist die Nutzung des Internets für private Zwecke nur dann ausgeschlossen, wenn die Interessen des Arbeitgebers gefährdet oder die Arbeitspflicht des Arbeitnehmers verletzt werden[208]. Eine Überwachung und Kontrolle der Mitarbeitenden sind in diesen Fällen nur bei Vorliegen von konkreten Hinweisen auf die Verletzung der Treuepflicht erlaubt[209]. Die Einwilligung des Arbeitgebers, dass die Internetnutzung für private Zwecke während der Arbeitszeit erlaubt ist, lässt auf die Respektierung der Privatsphäre der Arbeitnehmer vertrauen[210].

Wenn die Kontrollrechte durch den Arbeitgeber verletzt werden, stehen dem Arbeitnehmer die allgemeinen Rechtsansprüche und Verfahrensmittel nach Art. 15 DSG in Verbindung mit Art. 28 – 28l ZGB zur Verfügung[211].

3.1.5. Rechtsprechung

Die Überwachung durch Arbeitgeber war in den vergangenen Jahren Thematik sowohl in der nationalen wie auch europäischen Rechtsprechung. Das Bundesgericht hielt eine fristlose Kündigung als ungerechtfertigt, da der Arbeitgeber die Beweise mittels eines geheimen Überwachungsprogramms erlangte und diese somit nicht verwertbar waren[212].

[205] SHK EAV-GORDON/NEUENSCHWANDER/SCHMID, Art. 328b OR N 50; STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18; STUTZ/VALLONI, Rz. 5.47.
[206] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18; STUTZ/VALLONI, Rz. 5.47; WANTZ/LICCI, Rz. 26.
[207] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18.
[208] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18.
[209] STUTZ/VALLONI, Rz. 5.50.
[210] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18.
[211] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18.
[212] STUTZ/VALLONI, Rz. 5.47; Urteil BGer 8C_448/2012 vom 17. Januar 2013.

Mittels der Spyware wollte der Arbeitgeber beweisen, dass der Mitarbeiter die ihm zur Verfügung gestellten Mittel im Informatikbereich für dienstfremde Zwecke missbrauchte[213]. Die Verwendung von Spyware ist lediglich in Fällen denkbar, in welchen bei Vorliegen eines begründeten Verdachts die Aufklärung einer schweren Straftat notwendig wird, entschied das Bundesgericht[214]. In diesem Fall war der Einsatz der Software jedoch unverhältnismässig und wäre durch weniger drastische Massnahmen wie bspw. präventive Sperrung von Webseiten oder Analyse der Webnutzung nach Empfehlung des EDÖB zu lösen gewesen[215]. Das Bundesgericht hielt weiters in den Erwägungen fest, dass eine ständige elektronische Überwachung negative Auswirkungen auf die Gesundheit und das Wohlbefinden der Arbeitnehmer hat und diese in Stresssituationen versetzt, was sich negativ auf die Qualität der Arbeit auswirkt[216].

In einem anderen Fall ging es um einen fristlos entlassenen SBB-Mitarbeiter, welcher während 17 Tagen am Arbeitsplatz rund 80 Stunden Internetseiten mit pornografischem Inhalt konsumierte. Hier wurde die Verwertbarkeit der Beweise aus dem Internetverkehr und damit die Rechtmässigkeit der fristlosen Entlassung bejaht[217]. Die SBB hatte bei der Überwachung die Privatsphäre nicht systematisch verletzt, sondern war zu Beginn korrekt vorgegangen und hatte erst aufgrund eines Verdachts, welcher durch nicht-personenbezogen erhobene Daten bestätigt worden war, die IT-Aktivitäten personenbezogen analysiert[218]. Das Bundesgericht stellte in diesem Urteil auf qualitative und quantitative Kriterien ab, um die Verhältnismässigkeit einer anonymisierten Datenauswertung festzustellen[219]. Folgende qualitativen Merkmale bezüglich Art der missbräuchlichen Nutzung wurden dabei aufgeführt[220]:

- Schädigende Postings im Internet, welche den Ruf des Arbeitgebers gefährden;
- Die Verletzung der Geheimhaltungspflicht durch Verrat von Betriebs- und Geschäftsgeheimnissen im Internet;

[213] WILDHABER/HÄNSENBERGER, Kündigungsfalle, Rz. 36.
[214] WANTZ/LICCI, Rz. 26; Urteil BGer 8C_448/2012 vom 17. Januar 2013, E. 5.5.6.
[215] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 423.
[216] Urteil BGer 8C_448/2012 vom 17. Januar 2013, E. 5.5.3.
[217] PORTMANN/RUDOLPH, Art. 328b OR N 41; Urteil BGer 8C_79/2016 vom 30. Juni 2017.
[218] PORTMANN/RUDOLPH, Art. 328b OR N 41.
[219] Urteil BGer 8C_79/2016 vom 30. Juni 2017, E. 6.4; WILDHABER/HÄNSENBERGER, Urteil BGer 8C_79/2016, S. 1256.
[220] WILDHABER/HÄNSENBERGER, Urteil BGer 8C_79/2016, S. 1256.

- Das Herunterladen von Daten, welche Schadsoftware enthalten oder enthalten können;
- Cybermobbing von Arbeitskollegen;
- Die Gefährdung der IT-Systemsicherheit des Arbeitgebers;
- Oder den Arbeitgeber der Gefahr einer straf- oder zivilrechtlichen Haftung oder eines anderweitigen Risikos auszusetzen.

Der zeitliche Umfang der missbräuchlichen Nutzung an der Sollarbeitszeit kann als Massstab für den quantitativen Missbrauch dienen[221]. Dabei muss für jeden Einzelfall entschieden werden, welcher Umfang als missbräuchlich gilt. So betrug der zeitliche Umfang der Privatnutzung im SBB-Urteil rund 57 % und erfüllte das quantitative Kriterium. Hier erwähnenswert ist auch das Urteil des EGMR, welcher den Staat Rumänien rügte. Es kritisierte, dass der Staat keinen angemessenen Schutz des Rechts auf Achtung des Privatlebens und der Korrespondenz gewährte und es folglich unterliess, einen fairen Ausgleich zwischen den auf dem Spiel stehenden Interessen zu treffen. Die Gerichte versäumten es abzuklären, ob der damalige Beklagte über die Überwachung und auch deren Art und Umfang vorgängig informiert wurde und welche spezifischen Gründe die Einführung der Überwachungsmassnahmen rechtfertigten[222].

Diese Urteile zeigen die Bedeutsamkeit auf, dass Arbeitgebende zuerst alle organisatorischen, rechtlichen sowie technischen Massnahmen gegen eine missbräuchliche Nutzung des Internets umsetzen müssen, bevor sie eine Überwachung und Kontrolle der Internetzugänge vornehmen können[223]. Falls alle erforderlichen präventiven Massnahmen ergriffen wurden, können anonyme Überwachungsauswertungen durchgeführt werden. Erst als letzter Schritt darf bei gänzlich verbotener privater Nutzung oder bei festgestelltem Missbrauch eine personenbezogene Überwachung stattfinden[224].

3.2. Sanktionen und Rechtsfolgen

Sollte sich herausstellen, dass die Nutzung von sozialen Medien durch Mitarbeitende widerrechtlich erfolgte, stehen dem Arbeitgeber verschiedene Sanktionsmöglichkeiten zur Verfügung. Bei der Wahl ist darauf zu achten, welche Sanktion angemessen ist, um auf

[221] WILDHABER/HÄNSENBERGER, Urteil BGer 8C_79/2016, S. 1256.
[222] EGMR, Urteil vom 5. September 2017, Bărbulescu/Rumänien, Nr. 61496/08, E. 140/141.
[223] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 424.
[224] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 424.

den entsprechenden Verstoss zu reagieren. Sind in einem Reglement Sanktionsstufen festgehalten, so ist nach diesen vorzugehen.

3.2.1. Verwarnung

Bei geringfügigem Missbrauch gegen die arbeitsrechtlichen Weisungen empfiehlt sich, den Mitarbeiter abzumahnen[225]. Dabei sind unmissverständlich das Fehlverhalten zu rügen sowie die Konsequenzen im Wiederholungsfalle aufzuzeigen. Es ist zu empfehlen, die Verwarnung im Rahmen eines persönlichen Gesprächs mit dem Mitarbeitenden auszusprechen und ihm bei dieser Gelegenheit die Verwarnung schriftlich zu übergeben. Der Empfang der Verwarnung sollte durch den Mitarbeiter schriftlich bestätigt werden. Dies ist wichtig als Beweismittel, falls es bei der Fortführung der Zusammenarbeit zu weiteren Problemen kommt und schärfere Sanktionsmassnahmen notwendig werden. Eine Verwarnung ist dann ein sinnvolles Sanktionsinstrument, wenn vom Arbeitnehmer eine Verhaltensänderung erwartet werden und er diese selbst beeinflussen kann.

3.2.2. Lohnausfall

Erfolgt eine private Internetnutzung in einem derartigen Umfang, dass von einer Arbeitsleistung im Interesse des Arbeitgebers nicht mehr die Rede sein kann, so schuldet der Arbeitgeber dem Arbeitnehmer für den fraglichen Zeitraum keinen Lohn[226]. Entsprechend kann er eine Lohnkürzung vornehmen. Diese Sanktion ist jedoch aus Arbeitgebersicht schwierig durchzusetzen, da er beweisen muss, in welchem Zeitraum und für welche Dauer der Missbrauch stattgefunden hat[227]. Infolge der Hindernisse für die präventive Überwachung (s. Kapitel 3.1) kommt diese Sanktion kaum zur Anwendung.

3.2.3. Kündigung

Eine Kündigung nach Art. 335 OR ist bei schweren Verstössen infolge der Kündigungsfreiheit grundsätzlich zulässig[228]. Bei Anfechtung der Kündigung, welche auf eines der in Kapitel 2 beschriebenen Risiken begründet, trägt der Arbeitgeber die Beweislast für die arbeitsrechtliche Pflichtverletzung[229]. Hier stösst dieser auf das Problem, wie er Beweise vorlegen kann, welche nicht das Persönlichkeitsrecht des Arbeitnehmers verletzen.

[225] STUTZ/VALLONI, Rz. 5.32.
[226] STUTZ/VALLONI, Rz. 5.36; WILDHABER/HÄNSENBERGER, Internet, S. 314 f.
[227] EGLI, Soziale Netzwerke, Rz. 52.
[228] STUTZ/VALLONI, Rz. 5.32.
[229] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 421.

So stützte das OGer ZH im Berufungsverfahren den Entscheid der Vorinstanz, welche eine fristlose Kündigung als ungerechtfertigt einstufte. Geurteilt wurde, dass das Interesse an der Wahrheitsfindung gegenüber dem Schutz der Geheimsphäre der Klägerin nicht überwog, weshalb das rechtswidrig beschaffte Beweismittel (Screenshots von Chatverläufen) nicht berücksichtigt werden konnte[230].

Wird eine Kündigung gerichtlich als missbräuchlich nach Art. 336 OR beurteilt, ist dem entlassenen Mitarbeiter der gesamte Lohn während der ordentlichen Dauer der Kündigungsfrist geschuldet sowie nach Art. 336a OR eine Entschädigung von bis zu sechs Monatslöhnen zu bezahlen[231]. Nicht missbräuchlich sind bspw. Kündigungen bei Meinungsäusserungen von Mitarbeitenden, wenn diese eine Pflicht aus dem Arbeitsverhältnis verletzen oder die Zusammenarbeit im Betrieb wesentlich beeinträchtigen (Art. 336 Abs. 1 lit. b OR). Grobe Beleidigungen des Arbeitgebers, der Arbeitskollegen, der Kunden oder Geschäftspartner des Arbeitgebers, die nach Inhalt und Form zu einer erheblichen Ehrverletzung der Betroffenen führen, können deshalb eine ordentliche und nicht missbräuchliche Kündigung nach sich ziehen[232].

Vorsicht geboten ist bei fristlosen Kündigungen nach Art. 337 OR, welche bei besonders schwerwiegenden und mutwilligen Verstössen angewendet werden kann. Ob ein dafür notwendiger wichtiger Grund nach Art 337 Abs. 2 OR vorliegt, ist im Einzelfall abzuklären. Hierzu ist zu berücksichtigen, ob der Arbeitgeber klare Anordnungen zur Benutzung der elektronischen Kommunikationsmittel erlassen hat und ob er sich früher bereits eindeutig gegen die missbräuchliche Nutzung des Internetzugangs oder sogar diesbezügliche Verweise und Verwarnungen ausgesprochen hatte[233]. Auch weitere Elemente, insbesondere die Stellung und Verantwortung des Arbeitnehmers, die Art und Dauer des Vertragsverhältnisses sowie Art und Umfang der Verstösse sind miteinzubeziehen[234].

3.2.4. Strafrechtliche Konsequenzen

Auch von strafrechtlicher Seite kann bei widerrechtlicher Nutzung von sozialen Medien Ärger drohen. Dieser kann nicht nur den Arbeitnehmer treffen, sondern auch den Arbeitgeber selbst. Die Nutzung des Internetzugangs hinterlässt eine Datenspur im Internet.

[230] OGer ZH, Entscheid vom 20. März 2019, LA1800031-O-U, E. 3 ff.
[231] STUTZ/VALLONI, Rz. 5.32.
[232] WILDHABER/HÄNSENBERGER, Internet, S. 313.
[233] WILDHABER/HÄNSENBERGER, Internet, S. 314.
[234] BGE 127 III 310, E. 3.

Diese kann anhand der IP-Adresse dem Arbeitgeber zugeordnet werden, wodurch dieser in den Fokus der Strafverfolgungsbehörden geraten kann, wenn der Zugang für widerrechtliche Aktivitäten verwendet wurde[235]. Deliktsfähig sind jedoch lediglich die natürlichen, nicht die juristischen Personen[236]. Dem Arbeitgeber obliegt keine permanente Nachforschungspflicht nach möglichen Straftaten. Die Geschäftsleitung eines Unternehmens muss jedoch bei Vorliegen konkreter Hinweise zu einer möglichen Straftat den Indizien nachgehen, wenn sie eine persönliche Verantwortlichkeit vermeiden will[237].
Als strafrechtliche Tatbestände gelten[238]:

- Üble Nachrede (Art. 173 StGB)
- Verleumdung (Art. 174 StGB)
- Beschimpfungen (Art. 177 StGB)
- Konsum oder Zugänglichmachen von qualifiziertem pornografischem Material (Art. 197 Abs. 4 und 5 StGB)
- Rassendiskriminierung (Art. 261bis StGB)
- Verbreiten anderweitig illegaler Inhalte
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB)
- Unbefugte Datenbeschaffung (Art. 143 StGB)
- Urheberrechtsdelikte (Art. 71 URG) (Nebenstrafrecht)
- Wettbewerbsdelikte (Art. 26 UWG) (Nebenstrafrecht)

Auf die strafrechtlichen Konsequenzen wie bspw. Geldstrafe oder Freiheitsstrafe wird in dieser Arbeit nicht vertiefter eingegangen.

3.2.5. Schadenersatz

Verletzt der Mitarbeitende durch die Nutzung von sozialen Medien seine Treuepflicht nach Art. 321a Abs. 1 OR, kann der Arbeitgeber auch eine Schadenersatzforderung gegenüber dem Arbeitnehmer geltend machen[239]. Für die Haftung des Arbeitnehmers gelten folgende Voraussetzungen[240]:

[235] STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 17; WILDHABER/HÄNSENBERGER, Internet, S. 315.
[236] HOLENSTEIN, S. 43.
[237] HOLENSTEIN, S. 44.
[238] WILDHABER/HÄNSENBERGER, Internet, S. 315.
[239] WILDHABER/HÄNSENBERGER, Internet, S. 314.
[240] REHBINDER/STÖCKLI, Art. 321e OR N 21; SHK EAV-MILANI, Art. 321e OR N 5.

- Vertragsverletzung[241]
- Tatsächlich entstandener Schaden[242]
- Adäquater Kausalzusammenhang zwischen der Vertragsverletzung und dem entstandenen Schaden[243]
- Verschulden des Arbeitnehmers[244]

In der Lehre und Rechtsprechung haben sich Regeln für die Bestimmung des Schadenersatzes abgeleitet[245]. Das Mass des Verschuldens richtete sich dabei nach der Form der Fahrlässigkeit[246]:

Tabelle 5: Faustregeln zur Festsetzung des Schadenersatzes[247]

Verschulden	**Schadenzuführung**	**Merksatz**	**Faustregel für Haftungsumfang**
Absicht	Wissen und Wollen oder bewusstes Inkaufnehmen.	Das ist mit voller Absicht geschehen oder in Kauf genommen worden.	Schadenersatzpflicht in voller Höhe.
Grobe Fahrlässigkeit	Missachtung elementarster Sorgfalt und Vorsichtsmassnahmen.	Das darf einfach nicht passieren! Wie kann man nur?	Grundsätzlich keine Reduktion, Maximalhaftung in Höhe von drei Monatslöhnen.
Mittlere Fahrlässigkeit	Verletzung von Sorgfaltspflichten, aber ohne Missachtung elementarster Vorsicht.	Das sollte (eigentlich) nicht passieren.	Hälfte bis 2/3 des Schadens[248] maximal zwei Monatslöhne.
Leichte Fahrlässigkeit	Ausserachtlassen der gebotenen Sorgfalt.	Das kann schon mal passieren, aber man hätte besser aufpassen müssen.	Bis zur Hälfte des Schadens[249] maximal einen Monatslohn.

[241] SHK EAV-MILANI, Art. 321e OR N 8 f.
[242] SHK EAV-MILANI, Art. 321e OR N 6 f.
[243] SHK EAV-MILANI, Art. 321e OR N 10.
[244] SHK EAV-MILANI, Art. 321e OR N 11 ff.
[245] ROBERTO/SCHISTER, S. 393.
[246] REHBINDER/STÖCKLI, Art. 321e OR N 25; STREIFF/VON KAENEL/RUDOLPH, Art. 321e OR N 2.
[247] MEIER-GUBSER, Haftung, S. 293.
[248] a.M. ROBERTO/SCHISTER, S. 393, Hälfte des Schadens.
[249] a.M. ROBERTO/SCHISTER, S. 393, max. 10 – 20 % des Schadens.

Diese Faustregeln sollen jedoch nur als erste Einordnungshilfe verstanden werden, entscheidend sind stets die Umstände im Einzelfall[250]. Bei absichtlicher Schädigung erfolgt keine Reduktion der Schadenersatzpflicht[251]. Die Höchstgrenze der Schadenersatzpflicht ist gesetzlich nicht geregelt und wird von den Gerichten in einzelnen Entscheiden auch überschritten[252].

Ersatzforderungen für absichtlich zugefügten Schaden dürfen gemäss Art. 323b Abs. 2 OR mit dem Lohn des Arbeitnehmers verrechnet werden. Zu erwähnen ist hierbei, dass es eher selten zu Schadenersatzklagen durch Arbeitgeber kommt. Dies ist vor allem der Tatsache geschuldet, dass die Haftungssummen der Arbeitnehmer im Vergleich zu den Kosten und dem zeitlichen Aufwand, die durch ein entsprechendes Verfahren entstehen, eher bescheiden ausfallen.

3.3. Unternehmensinterne Präventivmassnahmen

3.3.1. Social-Media-Richtlinien

3.3.1.1. Erstellung der Richtlinien

Gerade bei der Fülle von Risiken und Themenfelder, welche die Nutzung der sozialen Medien im Arbeitsverhältnis bietet, sollten Arbeitgeber ihr Weisungsrecht nach Art. 321d OR nutzen und hierzu allgemeine Anordnungen erteilen[253]. Die Erstellung von sogenannten Social-Media-Richtlinien bezweckt das Minimieren der verschiedenen unter Kapitel 2 genannten Risiken. Mit einem Regelwerk zu dieser Thematik soll auch die Sensibilisierung der Mitarbeitenden erreicht werden, da sich diese oftmals der Folgen ihres Verhaltens in den sozialen Medien nicht bewusst sind[254]. Auch wird durch das Aufsetzen von einer Regelungen Rechtssicherheit und Transparenz geschaffen[255]. Bereits im 2005 erkannte das Unternehmen IBM, dass die Einführung einer Richtlinie zu einer offeneren, kollaborativeren und effizienteren Kommunikation führte, was sich positiv kritisch auf die Geschäftsstrategie und Förderung von Innovationen auswirkte[256].

[250] PORTMANN/RUDOLPH, Art. 321e OR N 18; ROBERTO/SCHISTER, S. 394; STREIFF/VON KAENEL/RUDOLPH, Art. 321e OR N 12.
[251] STREIFF/VON KAENEL/RUDOLPH, Art. 321e OR N 2.
[252] REHBINDER/STÖCKLI, Art. 321e OR N 31; STREIFF/VON KAENEL/RUDOLPH, Art. 321e OR N 12.
[253] PORTMANN/RUDOLPH, Art. 321d OR N 1; REHBINDER/STÖCKLI, Art. 321d OR N 3.
[254] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 427.
[255] STUTZ/VALLONI, Rz. 5.42.
[256] SCIACCA, S. 61.

Durch die Einführung einer entsprechenden Richtlinie geht es also nicht nur darum, die Mitarbeiter in der Nutzung einzuschränken, sondern diese soll auch als Hilfsmittel für eine effektive Unternehmenskommunikation dienen. Die Regelung zum Umgang mit den sozialen Medien kann bspw. in Form von Zusatzvereinbarungen zum Arbeitsvertrag, einer Betriebsordnung, Internet- und Social-Media-Guidelines oder anderen Regelwerken erfolgen[257]. Wichtig ist, dass nicht einfach ein unverbindlicher Leitfaden erstellt wird, sondern konkrete Regelungen erlassen werden. Dies ist unabdingbar, um bei Verstössen entsprechend handeln und Sanktionen umsetzen zu können[258].

Die Richtlinien sollen klare Informationen enthalten und auf diese Weise die Mitarbeitenden in die Verantwortung nehmen. Dabei sind nicht nur die Zulässigkeit und Begrenzung der Nutzung der sozialen Medien zu regeln, sondern auch Handlungsvorgaben für einen verantwortungsvollen Umgang auf Social Media aufzuführen[259]. Der Inhalt soll zum Nachdenken einladen und den Arbeitnehmern helfen, ihr Kommunikationsverhalten so zu gestalten, dass dieses mit den Werten des Unternehmens harmoniert. Hilfreich ist, wenn mit Beispielen veranschaulichen wird, was erlaubt ist und was nicht. Handlungsempfehlungen können auch unverbindlich für den privaten Bereich festgehalten werden. So kann eine entsprechende Sensibilisierung für eine verantwortungsbewusste Nutzung im Privatbereich erreicht werden, ohne dass unzulässig in das Recht auf freie Meinungsäusserung eingegriffen wird[260]. Damit die Verbindlichkeit der Richtlinie erreicht werden kann, ist es zwingend notwendig die Mitarbeitenden, insbesondere auch neu eintretende Mitarbeitende, über deren Existenz ausführlich zu informieren[261].

3.3.1.2. Inhalt der Richtlinien

Das Regelwerk zur Nutzung der sozialen Medien im Arbeitsverhältnis sollte u.a. folgende Punkte aufgreifen[262]:

- Definition des Zwecks einer solchen Richtlinie
- Geltungsbereich der Richtlinie
- Interessen und Risiken des Arbeitgebers

[257] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 427.
[258] PORTMANN/RUDOLPH, Art. 321d OR N 10 ff.; SHK EAV-MILANI, Art. 321d OR N 43f.
[259] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 427.
[260] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 427.
[261] PORTMANN/RUDOLPH, Art. 321d OR N 2; REHBINDER/STÖCKLI, Art. 321d OR N 6 f.
[262] EDÖB, Leitfaden Internet- und E-Mailüberwachung, Anhang B; STUTZ/VALLONI, Rz. 5.41; WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 429.

- Interessen und Risiken des Arbeitnehmers
- Technische Schutzmassnahmen und Protokollierung
- Nutzungsregelung
  - Inwieweit ist die private Nutzung der sozialen Medien gestattet?
  - Inwieweit ist die Nutzung der sozialen Medien während der Arbeitszeit und mittels betrieblicher Informatikinfrastruktur sowie mit privaten Geräten gestattet?
  - Aufzählung absolut verbotener Aktivitäten wie z.B. Konsumation von schädigenden Inhalten (bspw. pornografische Inhalte), Verbot an Beteiligung von Gruppen mit schädigenden Zwecken.
  - Verpflichtung zur wahrheitsgemässen Darstellung sowie zur Korrektur von falschen Angaben, wenn das eigene Unternehmen dargestellt wird oder betroffen ist.
  - Verbot der Offenlegung von Betriebs- und Geschäftsgeheimnissen und Verletzung von geistigem Eigentum.
  - Pflicht zur expliziten Kennzeichnung privater Meinungen (z.B. Verwendung von «ich» statt «wir», zusätzlich sollte bei der privaten Nutzung die Verwendung der Firmen-E-Mail-Adresse zur Anmeldung bei sozialen Medien untersagt werden, um eine Zurückverfolgung zum Unternehmen zu verhindern.).
  - Generelle Pflicht zur Einhaltung der geltenden Gesetze wie bspw. strafrechtliche und urheberrechtliche Bestimmungen.
- Überwachungsregelung / Kontrollrechte des Arbeitgebers
- Auflistung der Sanktionen bei Verstössen
- Behandlung der Accounts und der über berufliche soziale Netzwerke geknüpften Kontakte bei Anstellungsende

3.3.1.3. Rechtliche Auswirkungen der Richtlinien

Erlässt ein Unternehmen keine Nutzungsregeln, kann ihm vorgeworfen werden, dass es nicht genügend Massnahmen gegen einen möglichen Missbrauch der Nutzung von elektronischen Kommunikationsmitteln ergriffen hat[263]. Auswirkungen hätte dies insbesondere auf die personenbezogenen Überwachungsmöglichkeiten und Kontrollrechte des Arbeitgebers (s. Kapitel 3.1)[264]. Dies würde in einem solchen Fall gegen die

[263] WILDHABER/HÄNSENBERGER, Internet, S. 340.
[264] STUTZ/VALLONI, Rz. 5.43; WANTZ/LICCI, Rz. 43.

Verhältnismässigkeit nach Art. 4 Abs. 2 DSG sprechen. Die Erforderlichkeit der Überwachungsmassnahmen ist bei fehlender Anordnung kaum gegeben, da eine gleich geeignete, aber mildere Massnahme, nämlich der Erlass einer Nutzungsregelung, für den angestrebten Erfolgt zumeist ausreichen würde[265].

Zu beachten ist, dass eine pauschale Einwilligung, wonach der Arbeitgeber über alle Daten auf seinem System zu geschäftlichen Zwecken verfügen kann, unzulässig ist, auch wenn diese durch Annahme eines entsprechenden Reglements erfolgte[266].

3.3.2. Technische Präventivmassnahmen

Der Einsatz von Firewalls und Antivirusprogrammen ist unabdingbar. Arbeitgeber können durch technische Sperrungen den Zugriff auf Social-Media-Plattformen oder den Download bestimmter Dateien verunmöglichen. Der Nutzen, der durch das Sperren von Social-Media-Seiten im Unternehmensnetzwerk erreicht werden kann, ist jedoch nur beschränkt. Im Zeitalter von Smartphones ist es für Mitarbeitende problemlos möglich, ihre Aktivitäten während der Arbeitszeit über das private Gerät zu verrichten. Immerhin könnte durch technische Sperrungen im Unternehmensnetzwerk zumindest das Risiko der IT-Sicherheit für die firmeneigenen Geräte teilweise erreicht werden. Alle weiteren Risiken können durch diese Massnahme jedoch nicht unterbunden werden.

Gaben 2012 im Swiss Social-Media-Report der ZHAW noch 38 % der befragten Unternehmen an, sie hätten für die Mitarbeitenden den Zugang auf Facebook gesperrt, wird die Sperrung in der Studie von 2020 überhaupt nicht mehr thematisiert. Es ist nun reine Spekulation dies so zu interpretieren, dass technische Vorkehrungen nicht mehr zeitgemäss sind.

Für Accounts, welche die Firma repräsentieren, sollte der Zugang beschränkt und nur für eine übersichtliche Anzahl von Mitarbeitenden möglich sein. Mitarbeitende sollten regelmässig darauf aufmerksam gemacht werden, sichere Passwörter sowie, wo möglich, Multi-Faktor-Authentifizierungen zu verwenden.

[265] WILDHABER/HÄNSENBERGER, Internet, S. 340.
[266] WANTZ/LICCI, Rz. 45.

4. Diskussion / Schlussfolgerungen

4.1. Erkenntnisse

4.1.1. Spannungsfeld für Unternehmen

Wie die vorherigen Kapitel aufzeigen, sind Arbeitgeber mit vielfältigen Risiken bei der Nutzung von sozialen Medien im Arbeitsverhältnis konfrontiert. Dabei sehen Unternehmen die grössten Herausforderungen bei Themen wie Datensicherheit, Sorge vor Shitstorms, kollektiver Empörung und eskalierenden Situationen[267]. All diese Gefahren können zu erheblichen Reputationsproblemen führen und sich mitunter für Unternehmen als lebensbedrohend erweisen.

Unternehmen sind in der gesamten Thematik von verschiedenen Konfliktsituationen betroffen. Welche rechtlichen Interpretationen gelten bspw., wenn es um die Nutzung während der Arbeitszeit geht? Die gesetzlichen Rahmenbedingungen sowie Bundesgerichtsurteile zur Überwachung stellen für Arbeitgeber einerseits grosse Hürden dar. Andererseits sind Arbeitgeber verpflichtet, bei Untersuchungen in Bezug auf Verdacht auf Cybermobbing oder entehrenden Äusserungen gegenüber Dritten oder anderen Arbeitnehmer ebensolche Massnahmen anzuwenden. Die Anwendung der Untersuchungsstufen der Überwachung (s. Kapitel 3.1.4) ist komplex und ein Fehlverhalten kann dem Arbeitgeber bei einem Gerichtsverfahren angelastet werden.

Zudem sind Arbeitgeber durch die Entwicklungen in Bezug auf neue Arbeitsformen und der Verlagerung der Arbeit ins Homeoffice, ausgelöst durch die COVID 19-Pandemie, gefordert. Diese neuen Arbeitssituationen können bei Unternehmen ein erhöhtes Kontroll- und Überwachungsbedürfnis hervorrufen.

Personalmarketing sowie Arbeitgeberimage werden weiterhin wichtige Themen sein, die vermehrt über soziale Medien stattfinden werden.[268] Aber auch Influencer, im Personalmarketingkontext besonders interne Influencer, werden an Bedeutung gewinnen und von Unternehmen gezielt in der Personalarbeit eingesetzt.

[267] Bernet ZHAW Studie, S. 6.
[268] Bernet ZHAW Studie, S. 25.

4.1.2. Rechtliche Problematiken

Viele Fragen im Zusammenhang mit der Nutzung von sozialen Medien am Arbeitsplatz können nicht einfach mit Ja oder Nein beantwortet werden. Die Meinungen dazu in der Fachwelt sind unterschiedlich und teilweise werden Themen und Risiken divers interpretiert. Beispiele hierfür sind die Nutzung während der Arbeitszeit oder auch Teile der Überwachungsthematik. Dieser gesetzliche Graubereich erschwert es Arbeitgebern, sich an den rechtlichen Vorgaben zu orientieren.

Die gerichtliche Durchsetzung von Ansprüchen wird durch Arbeitgeber kaum verfolgt. Der Rechtsweg wird meist erst in Extremfällen beschritten. Dies ist vor allem den Faktoren Zeit und Geld geschuldet. Der Schaden, welcher durch Social-Media-Posts entstehen kann, tritt schnell ein. Gerichtsverfahren dauern in der Regel lange. Bis ein Gerichtsverfahren über einen entsprechenden Fall geurteilt hat, ist die öffentliche Meinung gebildet und das Image auch durch ein Urteil nicht mehr zu retten. Die Einforderung von Schadenersatz macht auch aus finanzieller Sicht kaum Sinn. Wie bereits in Kapitel 3.2.5 erwähnt, decken die Haftungssummen meist bei weitem nicht den entstandenen Schaden, geschweige denn den zeitlichen und finanziellen Aufwand der Verfahren.

Eine weitere Problematik auf der rechtlichen Seite ist auch, dass die Rechtsnormen nicht mit den Entwicklungen Schritt halten. Insbesondere zu Herausforderungen, welche neue Phänomene wie Corporate Influencer oder People Analytics mit sich bringen, fehlt eine eindeutige rechtliche Beurteilung.

4.1.3. Compliance-Thematik

Welches die nächsten Trends bei Social Media sind und welche neuen damit verbundenen Probleme auftauchen, wird die Zukunft zeigen. Gewiss ist, dass in dieser Technologie eine stetige Weiterentwicklung stattfinden wird, welcher sich Unternehmen wie auch Privatpersonen kaum entziehen können. Dass Unternehmen fortwährend mit neuen Herausforderungen in der Social-Media-Welt konfrontiert sein werden, zeigt auch ein aktuelles Gerichtsurteil aus den USA. Credit Suisse und UBS wurden von den amerikanischen Gerichtsbehörden nebst weiteren Grossbanken zu Millionenbussen verurteilt, weil sie die Kommunikation über Kurznachrichtendienste nicht gesichert hatten[269]. Dieses

[269] METTLER JON, Millionenbusse für CS und UBS in den USA, Tagesanzeiger Online vom 28. September 2022, <https://www.tagesanzeiger.ch/nach-millionenbusse-cs-aktien-im-freien-fall-621744372121>, besucht am: 30.09.2022.

Unterlassen verstösst in den USA gegen die Auflage, dass Bücher und Aufzeichnungen eines Unternehmens durch die US-Börsenaufsicht überprüfbar sein müssen. Eine Problematik, die bis anhin kaum jemand auf der Agenda hatte und plötzlich für finanziellen Schaden sowie schlechte Reputation sorgt. Solche Compliance-Verstösse können für die verantwortlichen Unternehmensleitungen schwerwiegende Folgen mit sich bringen. Gelten bspw. Arbeits- und Sozialversicherungsrecht, Kartellrecht, Buchführungsrecht, Steuerrecht etc. für jedes Unternehmen, gibt es je nach Branche auch weitere Compliance-Bereiche, die zu berücksichtigen sind. So haben bspw. die Finanzindustrie mit der Finanzmarktkontrolle und Geldwäschereigesetzgebung oder die Industrie mit der Exportkontrolle, Produktesicherheit etc. weitere Rechtsnormen einzuhalten[270].
Um sich vor Folgen gegen Compliance-Verstösse zu schützen, ist es für Unternehmen ratsam, umfassende Compliance-System etabliert zu haben. Diese umfassen den Erlass von Weisungen (Code of Conduct), die Schulung der Mitarbeitenden, das Einrichten von Anlaufstellen sowie interne Untersuchungen und Sanktionen bei Compliance-Fällen. Auch People Analytics/Workforce Analytics kann die rechtliche Compliance unterstützen. Dies bspw. bezüglich der Überprüfung der Einhaltung von Arbeitszeiten oder Sicherheitsvorgaben.

4.1.4. Herausforderungen der Zukunft

4.1.4.1. Technologische Trends

Die Anwendung von Algorithmen befindet sich erst noch in der Anfangsphase. Es ist anzunehmen, dass sich diese technische Art der Personalsteuerung, insbesondere bei internationalen Grossunternehmen, stärker etablieren wird.
Im Vergleich zum Metaverse erscheint die Social-Media-Welt bereits wieder überholt. Über unsere Smartphones und Social-Media-Accounts leben wir in einer Art Parallelwelt. Mit dem Metaverse steht das nächste Level der Digitalisierungsentwicklung in den Startlöchern, um die Gunst der Nutzer zu erobern. Erste finanzstarke und innovative Unternehmen haben bereits ihre Firma als eigene Metaverse-Version erschaffen. So hat zum Beispiel das koreanische Elektronikunternehmen Samsung eine virtuelle Rekrutierungsmesse veranstaltet und der Autohersteller Hyundai hat das Metaverse für das Onboarding

[270] EGLI URS, e:4.15 Compliance, <https://www.epartners.ch/pub/e-4-15-compliance>, besucht am: 21.10.2022.

neuer Mitarbeiter genutzt. Auch die britische Niederlassung von PwC nutzt die Technologie in der Rekrutierung von neuen Mitarbeitenden und schuf eine Metaverse-Plattform, um Bewerber zu interviewen[271]. Diese Beispiele zeigen, dass die Digitalisierung noch längst nicht an eine Grenze gelangt ist. Auch diese Entwicklung wird wieder neue Risiken zu Tage bringen, auf welche Unternehmen sich einstellen und vor ihnen schützen müssen.

4.1.4.2. Ausblick Gesetzgeber

Die Veränderungen in der Arbeitswelt, seien dies bspw. neue Arbeitsformen oder der Einsatz von digitalen Hilfsmitteln, werden auch zu neuen Herausforderungen im Arbeitsrecht führen. Spannend wird sein, ob und wie sich die arbeitsrechtliche Gesetzgebung in den kommenden Jahren verändern wird. Durch den Wegfall der strikten Trennung von Arbeit und Privat, was auch durch die Nutzung von sozialen Medien häufig der Fall ist, wird bspw. die Anwendung des Arbeitsgesetzes für die Unternehmen eine grosse Herausforderung. Was gilt als Arbeits- und Freizeit und wie können die Regelungen bezüglich Ruhezeiten trotz der agiler werdenden Arbeitstätigkeit korrekt eingehalten werden? Selbstverständlich werden nicht alle Branchen im gleichen Ausmass mit dieser Problematik tangiert sein.

Es sieht so aus, dass vorerst keine grösseren Veränderungen auf Gesetzesebene anstehen. In seinem Bericht «Auswirkungen der Digitalisierung auf Beschäftigungen und Arbeitsbedingungen – Chancen und Risiken» vom 8. November 2017 hielt der Bundesrat fest, dass kein grundlegender Handlungsbedarf auf gesetzgeberischer Ebene vorliegt und die Bestimmungen hinsichtlich Arbeitsrecht, Datenschutz, Arbeitsmarktaufsicht, Arbeitssicherheit und Gesundheitsschutz ihren Zweck auch im veränderten Umfeld erfüllen. Bereits im 2013 wurde die Einführung eines speziellen Gesetzes für Social Media vom Bundesrat abgelehnt[272]. Den arbeitsrechtlichen Herausforderungen, welche durch die Digitalisierung weiter entstehen werden, ist im Wesentlichen mit den bestehenden Rechtsnormen zu begegnen[273]. Wegleitende Weichenstellungen, gerade im Bereich der Digitalisierungsfragen, werden folglich von den Gerichten zu fällen sein[274].

[271] VAN VULPEN ERIK, Three Ways The Metaverse Could Transform HR, Forbes Online vom 3. Juni 2022, <https://www.forbes.com/sites/forbeshumanresourcescouncil/2022/06/03/three-ways-the-metaverse-could-transform-hr/?sh=5b0df23f6db4>, besucht am: 30.09.2022.
[272] WILDHABER/HÄNSENBERGER, Kündigung wegen Nutzung, S. 400.
[273] RUDOLPH, S. 394-395.
[274] RUDOLPH, S. 396.

4.2. Empfehlungen

4.2.1. Kommunikative Sensibilisierung

Ein wichtiger Faktor für die Prävention von Risiken, ist die Sensibilisierung der Mitarbeitenden. Das blosse Aufsetzen einer Richtlinie zum Umgang mit sozialen Medien genügt dabei allein nicht, sich vor den Risiken zu schützen. Eine wichtige Massnahme, welche Mitarbeitende unbewusst wahrnehmen, ist ein positives Vorleben von Social-Media-Aktivitäten in der Unternehmenskommunikation. Für den Unternehmenserfolg ist eine Social-Media-Planung über alle Bereiche wertvoll. Eine Strategie, welche Zielgruppen sollen auf welchen Kanälen angesprochen werden, hilft auch den Mitarbeitenden, sich bei der Vielfalt der Plattformen nach bestem Nutzen und Zweck zu orientieren. Mitarbeitende nehmen dabei wahr, welche Kanäle das Unternehmen bespielt und in welcher Tonalität auf diesen kommuniziert wird.

Marketing- und Kommunikationsabteilungen müssen den korrekten Umgang mit sozialen Medien vorleben. Deren Mitarbeitenden sollten sich bewusst sein, dass ihre Arbeitsprozesse als Vorbild gelten. So sollte es selbstverständlich sein, dass von Mitarbeitenden vor Veröffentlichung von Beiträgen das Einverständnis von involvierten Personen oder der Unternehmenskommunikation eingeholt wird.

Einem Aufruf, die allgemeinen Geschäftsbedingungen der entsprechenden Plattformen zu konsultieren, werden Mitarbeitende kaum Folge leisten. Es wird sich wohl nur eine Minderheit die Zeit nehmen, mehrere Seiten an rechtlichen Inhalten zu lesen. Geschweige denn, dass der Inhalt solcher AGB für den Durchschnittsnutzer oftmals unverständlich ist. Hier ist es hilfreich, wenn durch die Kommunikationsabteilung in Zusammenarbeit mit der Rechtsabteilung die wichtigsten Informationen verständlich und ansprechend zusammengefasst werden. Dies setzt voraus, dass ein Unternehmen über die entsprechenden Ressourcen verfügt.

Allgemein einen wichtigen Nutzen würde die Schaffung einer Anlaufstelle für Social-Media-Fragen oder das Einführen von Social-Media-Coaches bringen.

4.2.2. Entwicklung Social-Media-Kompetenz

Ganz gezielt können die Mitarbeitenden auch mittels Schulungen sensibilisiert werden. Bereits beim Onboarding-Prozess sind die neuen Mitarbeitenden mit dem Social-Media-Kodex des Unternehmens bekannt zu machen. Vielleicht publiziert der eine oder andere

Mitarbeitende darauf einen positiven LinkedIn-Beitrag über seinen Stellenwechsel und macht auf diese Weise bereits Werbung für den neuen Arbeitgeber.
Ebenfalls sollten Führungskräfte eine explizite Schulung zu Social-Media-Themen und insbesondere der verschiedenen Risiken erhalten. Sie sind die Personen, welche am nächsten bei ihren Mitarbeitenden sind und meist vor den HR-Abteilung oder der Unternehmensleitung auf Problematiken aufmerksam werden resp. in solche involviert sind.
Zudem empfiehlt es sich, das Thema auch bezüglich der Weiterentwicklung der Mitarbeitenden auf der Agenda zu haben. Im Kompetenzmodell der Zukunft sind Social-Media-Fähigkeiten kaum weg zu denken. Mitarbeitende, welche im geschäftlichen Auftrag auf den sozialen Medien unterwegs sind, müssen fit in der Corporate Language und dem Berücksichtigen des Corporate Designs sein. Zudem sollten sie im Ansatz die gesetzlichen Vorgaben bezüglich Bildrechten, Musiklizenzen, Markenrechte etc. kennen, damit sie keine strafbaren Handlungen im Rahmen ihrer Tätigkeit für das Unternehmen vornehmen.
Ausführliche Informationen und gezielte Schulung der Mitarbeitenden kann die Hemmschwelle zur Nutzung von sozialen Medien deutlich verringern. Wichtig bei Schulungen ist es, die Ziele der einzelnen Plattformen und die damit einhergehenden Vorteile in der Informationsübermittlung und der Kollaboration hervorzuheben. Auf diese Weise kann die Akzeptanz bei den Mitarbeitenden gefördert werden. Tipps und Tricks zu Themen wie bspw. Fotoaufnahme über Mobilegeräte oder Reichweitensteigerung von Posts, können dabei die Begeisterung bei Mitarbeitenden wecken und sind auch für den Privatbereich nützlich. Bei der Schulung von Mitarbeitenden soll es gelingen, durch spannende Inhalte kombiniert mit den Vorgaben der Unternehmens-Guidelines für den Umgang mit sozialen Medien zu motivieren und nicht nur durch die Aufzählung von Verboten abzuschrecken. Technikaffine Mitarbeitende können als Early Adopters die neusten Trends auf den sozialen Medien ausprobieren und deren Erkenntnisse unternehmensweit teilen.
Die Social-Media-Kompetenz wird künftig eine viel grössere Rolle spielen als bisher. Egal ob es so weit gehen wird, dass Mitarbeitende als Corporate Influencer tätig sind. Know-how, wie erfolgreich auf den sozialen Medien kommuniziert wird und wie man sich erfolgreich vernetzt, wird für Unternehmen immer wichtiger. So ist es denkbar, dass sich diese Fähigkeit in den Kompetenzmodellen der Unternehmen wiederfindet und bei

der Rekrutierung von neuen Mitarbeitenden als wichtige Anforderungen eine grosse Rolle spielen wird.
Mitarbeitende, die sich dieser Technologie verschliessen, werden es künftig bei der Weiterentwicklung der Unternehmen schwer haben und auch deren Chancen auf dem Arbeitsmarkt verschlechtern sich.

4.3. Fazit

4.3.1. Beantwortung Forschungsfragen

Welche Resümees können nun in Bezug auf die Beantwortung der drei Forschungsfragen gezogen werden?

Hauptfrage	Mit welchen Risiken sind Arbeitgeber bei der Nutzung von sozialen Medien im Arbeitsverhältnis konfrontiert?

Wie vielseitig und zahlreich die verschiedenen Risiken infolge der Nutzung von sozialen Medien im Arbeitsverhältnis sein können, wurde in Kapitel 2 behandelt. Sie zeigen die häufigsten arbeitsrechtlichen Thematiken im Zusammenhang mit Social Media auf und sind nicht als vollständige Liste anzusehen. Jedes einzelne der Themen ist sehr vielschichtig und komplex.
Die Risikoexposition bei der Nutzung von sozialen Medien mit beruflichem Kontext ist nicht für alle Arbeitgeber gleich. Es ist unternehmensabhängig, ob und wie soziale Medien genutzt werden. Dabei spielen Faktoren wie die Unternehmenskultur, -grösse, Branche u.a. eine Rolle. Arbeitgeber sind einerseits mit expliziten Social-Media-Risiken wie Arbeitgeberbewertungsportale, rufschädigende Postings, Eigentumsverhältnisse von Accounts etc. konfrontiert. Andere Themen wie Verletzung der Geheimhaltungspflicht oder Cybermobbing resp. Mobbing sind Problematiken, welche auch aus der physischen Welt bekannt sind.
Das Online-Verhalten kann folglich auch mit dem physischen Alltagsverhalten verglichen werden, was teilweise auch in der Rechtsprechung erfolgt. Unterschiede gibt es jedoch in Bezug auf die Verbreitungsdimension wie auch die Beweise. Wenn bspw. Lästereien über die neue Geschäftsführung oder abfällige Äusserungen über Arbeitskollegen in der Kaffeepause stattfinden, hinterlässt dies keine physischen Spuren, nur Zeugen. Getätigte Äusserungen auf sozialen Medien hingegen hinterlassen Beweise und für die

Verfasser findet ein Kontrollverlust statt. Das Internet vergisst nicht und so besteht das Risiko, dass Posts zeitlich unbegrenzt abrufbar bleiben. Es sind die Schnelligkeit, der globale Zugang sowie der Interaktivitätsgrad, welche ein besonderes Augenmerk für einen bedachten Umgang mit sozialen Medien erfordern. Arbeitgeber, welche die verschiedenen Risiken kennen, können frühzeitig Gefahren identifizieren und sich rechtzeitig mit diesen auseinandersetzen.

Unterfrage 1	Wie gehen Arbeitgeber rechtlich korrekt bei Problemen bei der Nutzung von sozialen Medien durch Arbeitnehmende vor?

Die Durchsetzung von arbeitsrechtlichen Konsequenzen ist nie erfreulich. Bei aller Dringlichkeit und Aufregung, die sich meistens in solchen Situationen einstellen, ist ein reflektiertes Verhalten von Seiten Arbeitgeber unabdingbar. Gerade bei der Überwachung infolge von Verdachtsmomenten, ist ein rechtskonformes Vorgehen notwendig. Arbeitgeber sollten nicht infolge Missachtung von Vorschriften in die Kritik geraten. Es empfiehlt sich ein Vorgehen nach Eskalationsstufen definiert zu haben, welches Sicherheit im Aussprechen von Sanktionen gibt. Ebenfalls von Vorteil ist es, einen Notfallplan zur Hand zu haben, um einer Krisensituation umgehend und angemessen zu begegnen.
Arbeitgeber sollten sich bei schädigenden Äusserungen durch Mitarbeitende kritisch hinterfragen, wie es zur Situation gekommen ist. Kommentare auf sozialen Medien dienen oftmals als Ventil für Frustration und Ärger. Je nach Schwere des Verstosses ist der Dialog mit dem Verursacher zu suchen oder entsprechende Sanktionen anzuwenden.
Die Hürden für die Beschreitung des Rechtswegs sind aus Sicht Arbeitgeber hoch. Die Thematik liegt oftmals im rechtlichen Graubereich. Der zeitliche, finanzielle und auch nervliche Aufwand sprechen dafür, dass mit Arbeitnehmern möglichst aussergerichtliche Lösungen gesucht werden, bevor der Rechtsweg begangen wird.

Unterfrage 2	Durch welche Massnahmen lassen sich Risiken minimieren?

Zu den wichtigsten Massnahmen zur Prävention gehören die kommunikative Sensibilisierung der Mitarbeitenden sowie die Entwicklung deren Social-Media-Kompetenzen (s. Kapitel 4.2). Für Unternehmen lohnt es sich, in diese Thematiken zu investieren. Der potenzielle Schaden, der durch die Nutzung von sozialen Medien entsteht, kann sehr schnell unkontrollierbare Dimensionen annehmen, so dass sich Arbeitgeber plötzlich in

einem Albtraum wieder finden. Mitunter können Imageschädigungen zur Existenzbedrohung werden.

Basis für die Präventionsmassnahmen sind die Erstellung und Einführung von Social-Media-Richtlinien, welche entscheidenden Einfluss auf die arbeitsrechtlichen Instrumente haben. Technische Präventivmassnahmen hingegen eignen sich nicht für alle Unternehmen und weisen eher auf eine Misstrauenskultur eines Unternehmens hin. Mittels eines gezielten Social-Media-Monitorings können mögliche Krisen und Risiken schon in einem frühen Stadium erkannt werden. Dies erlaubt eine adäquate Reaktion in nützlicher Frist und kann allenfalls Probleme entschärfen, bevor sie sich zu einer Katastrophe entwickeln.

Aber nicht nur im Hinblick zur Risikoprävention zahlen sich diese Massnahmen aus. Investitionen in die digitale Kompetenz der Mitarbeitenden, werden für erfolgreiche Unternehmen unabdingbar. Bei dieser Thematik wegzuschauen oder sich passiv zu verhalten, wird sich für ein Unternehmen früher oder später nachteilig auswirken. Aus Compliance-Perspektive kann sogar behauptet werden, dass Unternehmen die Pflicht obliegt, sich mit diesem Themenbereich auseinanderzusetzen und klare Regelungen sowie eine Strategie für Mitarbeiterkommunikation und -schulung zu erarbeiten.

4.3.2. HR-Rolle

Den HR-Verantwortlichen kommt in der gesamten Thematik eine tragende Rolle zu. Eingebunden sowohl in Prävention wie auch in Sanktionsfällen, müssen HR-Abteilungen das Alphabet von sozialen Medien beherrschen. Wichtig sind vor allem Kenntnisse über die gesetzlichen Vorgaben, was bei der Vielfalt an betroffenen Rechtsgebieten durchaus herausfordernd sein kann. HR-Abteilungen sollten Unternehmensleitungen im Hinblick auf die Erarbeitung von Social-Media-Richtlinien und das entsprechende Kommunikationskonzept mitberaten. Nebst der HR-Abteilung sind diverse Bereiche wie IT, Marketing und Rechtsabteilung in die Gesamtthematik involviert und die Zusammenarbeit bildet den Grundstein für eine erfolgreiche Prävention. Dabei fällt der HR-Abteilung, wie schon deren Bezeichnung aussagt, auch die wichtige Aufgabe zu, die menschlichen Komponente zu berücksichtigen. Auch die HR-Abteilung sollte authentisch Social-Media-Aktivitäten pflegen und so als Multiplikator mitwirken und eine Vorbildrolle einnehmen.

Nebst all den Risiken und Problematiken, die in dieser Arbeit aufgeführt wurden, darf nicht vergessen werden, welchen Mehrwert die sozialen Medien Unternehmen bringen.

So sind diese Netzwerke nicht nur aus Marketingsicht äusserst spannend, sondern leisten einen wichtigen Beitrag im Bereich Wissensmanagement. Zudem wurde auch die Zusammenarbeit und Kommunikation innerhalb der Unternehmen auf eine neue Ebene gebracht. Die Thematik ist interessant, vielschichtig und es wert, sich vertieft mit ihr auseinanderzusetzen. Eins ist klar, an sozialen Medien führt kein Weg vorbei.