
Big Data am Arbeitsplatz

Datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen¹

GABRIEL KASPER/ISABELLE WILDHABER

Inhaltsübersicht

I.	Einleitung	190
II.	People Analytics in den verschiedenen Phasen des Arbeitsverhältnisses	194
	A. People Analytics in der Bewerbungsphase	194
	1. Überblick über die relevanten Rechtsfragen	194
	2. Einwilligung der bestehenden Arbeitnehmer zur Erstellung eines Wunschprofils	194
	3. Bearbeitung der Daten der Bewerber	200
	a) Eignungsabklärung anhand der vom Bewerber mitgeteilten Informationen	200
	b) Persönlichkeitsdurchleuchtung anhand der durch die Arbeitgeberin erforschten Informationen	204
	c) Frageverbot	209
	d) Diskriminierungsverbot	209
	B. People Analytics während des laufenden Arbeitsvertrags	210
	1. Überblick über die relevanten Rechtsfragen	210
	2. Abgrenzung Personen- und Sachdaten	211
	3. Abgrenzung allgemein zugänglicher und privater Personendaten	217
	4. Verhaltensüberwachung am Arbeitsplatz	221
	C. People Analytics nach Beendigung des Arbeitsverhältnisses	224
III.	Schlusswort	227
	Literatur	228

¹ Vorliegender Aufsatz steht im Zusammenhang mit einem aktuell laufenden Projekt des FAA-HSG der Universität St. Gallen im Rahmen des SNF NFP 75 zu Big Data. Das Projekt, an dem die Autoren mitwirken, trägt den von George Orwells Roman 1984 inspirierten Titel «*Big Brother* in Schweizer Unternehmen? Vertrauen, Daten und Privatsphäre im Job».

Abstract

Big Data hält Einzug in die privatrechtlichen Arbeitsverhältnisse. Der Begriff «People Analytics» beschreibt den Vorgang der Big-Data-Analysen und -Überwachungen am Arbeitsplatz. Eine (zu) enge Überwachung durch die Arbeitgeberin kann zu einer unrechtmässigen Persönlichkeitsverletzung führen. Die Autoren weisen auf offene datenschutz- und arbeitsrechtliche Fragen zur Privatsphäre beim Einsatz von People Analytics hin. Sie gehen dabei chronologisch vor, angefangen beim Bewerbungsverfahren, über das laufende Arbeitsverhältnis bis zur Beendigung desselben. Sie kommen zum Schluss, dass People Analytics insbesondere in den folgenden Bereichen rechtlichen Klärungsbedarf verursacht: Einwilligung im Arbeitskontext, Kriterien zur Eignungsabklärung, Persönlichkeitsdurchleuchtung, Abgrenzung von Personen- und Sachdaten, Abgrenzung allgemein zugänglicher und privater Daten sowie Verhältnismässigkeit der Verhaltensüberwachung am Arbeitsplatz.

I. Einleitung

*«Big Data ist die Herausforderung für die Privatsphäre im 21. Jahrhundert.»²
Prof. Jacob Strahilevitz, Sidley University of Chicago Law School*

Big Data hält Einzug in die privatrechtlichen Arbeitsverhältnisse: Neue, datenbasierte Formen der Personalsteuerung erheben vom Arbeitnehmer Daten in grossen Mengen, um sie mit Hilfe von Algorithmen in Echtzeit oder hoher Geschwindigkeit auszuwerten.³ Daraus resultieren Korrelationen⁴ und genaue Kennzahlen zu unzähligen Variablen über das Individuum.⁵ Weitgehend unterstützen die Big-Data-Analysen Personalentscheidungen, teilweise fällen sie sie anstelle eines menschlichen Vorgesetzten.⁶

² STRAHILEVITZ, 2021.

³ Zur Charakterisierung von Big Data anhand von vier Eigenschaften, den Vs: WESPI, 4–5, bzw. drei Vs: REINSCH/GOLTZ, 36; kritisch zum Begriff Big Data und der Definition über Vs: FEW: Basta, big data: It's time to say arrivederci, 27.06.2017, <<https://www.perceptualedge.com/blog/?p=2670>> (besucht am 06.04.2018).

⁴ PRIEUR, 1644; WEBER/OERTLY, N 3; BAERISWYL, 46.

⁵ Vgl. HOLTHAUS/PARK/STOCK-HOMBURG, 677.

⁶ DZIDA, 542.

Die Terminologie dieses datengetriebenen Personalwesens ist aufgrund der jungen Entwicklung der Technologien noch nicht gefestigt: Die Begriffe «**People Analytics**»⁷ und «HR Analytics»⁸ sind am weitesten verbreitet. «Workforce Analytics»,⁹ «Talent Analytics»,¹⁰ «Human Capital Analytics»,¹¹ «Workplace Analytics»¹² und weitere Bezeichnungen¹³ kommen ebenfalls vor. Aufgrund der starken Verbreitung von «People Analytics» schliessen wir uns für die vorliegende Abhandlung dieser Begriffswahl an.¹⁴ Gleichwohl beschreibt der Begriff «Workforce Analytics» den Vorgang der Big-Data-Analysen am Arbeitsplatz wohl genauer, da die «Workforce» (im Gegensatz zu «People») einen spezifischen Bezug zum Arbeitsplatz herstellt. Ausserdem umfasst sie die Auswertung der gesamten Arbeitskraft, die zum Erfolg des Unternehmens beiträgt (Festangestellte, Temporärmitarbeiter, Talente, nicht angestellte Vertragspartner, Freelancer, Outsourcing-Dienstleister), einschliesslich der künftig zu erwartenden wachsenden Zahl von Robotern am Arbeitsplatz.¹⁵

People Analytics **bezweckt** die Optimierung des Betriebsablaufs, gesteigerte Effizienz und Innovation,¹⁶ ebenso die Verbesserung der Mitarbeiterzufrie-

⁷ 948 Millionen Treffer bei einer Google-Suche nach «People Analytics» am 22.11.2018. Je nach Einstellungen der Suchmaschine kann die Trefferzahl variieren.

⁸ 796 Millionen Google-Treffer (vgl. FN 7).

⁹ 391 Millionen Google-Treffer (vgl. FN 7).

¹⁰ 238 Millionen Google-Treffer (vgl. FN 7).

¹¹ 103 Millionen Google-Treffer (vgl. FN 7).

¹² 103 Millionen Google-Treffer (vgl. FN 7).

¹³ Seltener: «Human Resource Intelligence», «New Control» (im Gegensatz zu klassischer Kontrolle), «Performance Management», «Workforce Science», «Workplace Surveillance», und, etwas genereller, «Monitoring» und «New Normal» (Letzteres als Bezeichnung der allgemeinen Digitalisierung der Gesellschaft).

¹⁴ Vgl. FN 7 und 9. Im SNF-Projekt verwenden wir den Begriff «People Management Analytics».

¹⁵ GUENOLE/FERRAR/FEINZIG, 6, 16–17.

¹⁶ AJUNWA/CRAWFORD/SCHULTZ, 743.

denheit,¹⁷ die Reduktion von Vorurteilen in Entscheidungsfindungen,¹⁸ mehr Objektivität¹⁹ und Diversität²⁰ im Unternehmen.

Die **Verbreitung** von People Analytics steigt: In der Schweiz benutzten 2018 knapp zwei Drittel (64,6 %) der Grossunternehmen datenbasierte Tools zur Analyse der Mitarbeiter.²¹ Ausländische Studien bestätigen dies teilweise: Knapp ein Drittel (32 %) der 2015 weltweit befragten Unternehmen²² und ein Viertel (26 %) der 2014 befragten deutschen Unternehmen²³ nutzten Big Data zur Unterstützung des Personalbereichs²⁴. Allein bei Lösungen für das Leistungsmanagement soll die Analytik-Industrie angeblich ein Marktvolumen von USD 11 Milliarden aufweisen.²⁵ Der Markt wird in den nächsten Jahren um Millionen von Produkten, Dienstleistungen und neuen Stellen wachsen.²⁶

¹⁷ NIKLAS/THURN, 1590.

¹⁸ REINSCH/GOLTZ, 46.

¹⁹ SNYDER, 251–252.

²⁰ WILSON/BELLIVEAU/GRAY, 32.

²¹ Im Rahmen der Studie der Autoren (FN 1) nahmen 158 Schweizer Grossunternehmen an einer 2018 durchgeführten Online-Umfrage teil, bei der sie gefragt wurden, ob sie bestimmte IT-basierte Tools zur Personalsteuerung anwenden. 35,4 % der Teilnehmenden gaben an, keine dieser Tools zu verwenden, während 64,6 % solche Tools einsetzten.

²² WILSON/BELLIVEAU/GRAY (FN 20), 8.

²³ BISSELS/MEYER-MICHAELIS/SCHILLER, 3042.

²⁴ Andere weisen eine geringere Verbreitung aus: CLAYTON RICH: Wanted: Data scientists with liberal arts training, The Economic Times vom 28.08.2016, <<https://economic.times.indiatimes.com/small-biz/hr-leadership/people/wanted-data-scientists-with-liberal-arts-training/articleshow/53884306.cms>> (besucht am 26.11.2018); Workforce Analytics stecke in den Kinderschuhen: CLASSEN/GÄRTNER, 39.

²⁵ AJUNWA/CRAWFORD/SCHULTZ, 769.

²⁶ REINSCH/GOLTZ, 37; globales Marktvolumen von USD 1.87 Milliarden bis 2025: Grand View Research: Workforce analytics market worth \$1.87 billion by 2025, CAGR: 16 %, 06.2017, <<https://www.grandviewresearch.com/press-release/global-workforce-analytics-market>> (besucht am 15.11.2018); globales Marktvolumen von rund USD 2.5 Milliarden bis 2026: Transparency Market Research: Workforce analytics market to reach US\$ 2,453.9 Mn by 2026, 10.08.2018, <<https://globenewswire.com/news-release/2018/08/10/1550382/0/en/Workforce-Analytics-Market-to-Rich-US-2-453-9-Mn-by-2026-Transparency-Market-Research.html>> (besucht am 15.11.2018); vgl. schon die prognostizierten Zahlen bis 2015 bei Bersin Josh: Big data in human resources: Talent analytics (People Analytics) comes to age, Forbes vom 17.02.2013,

Wie das Eingangs zitat mahnt, kommen mit People Analytics grosse **Herausforderungen** auf die involvierten Personen zu. Den Arbeitnehmern droht eine enge Überwachung durch die Arbeitgeberin, die in die Rolle eines Big Brother²⁷ schlüpfen kann. Umgekehrt bestehen auch für die Arbeitgeberin rechtliche Risiken und Unsicherheiten, weil sich das Recht in diesem Bereich ständig weiterentwickelt.²⁸ Arbeitsrecht (Art. 328, Art. 328b OR), Datenschutz (DSG), Gesundheitsschutz (Art. 6 ArG, Art. 26 ArGV 3) und Persönlichkeitsschutz (Art. 27–28 ZGB) stellen kumulativ geltende Anforderungen an die Überwachung am Arbeitsplatz.²⁹

Die Autoren weisen auf offene **datenschutz- und arbeitsrechtliche Fragen** zur Privatsphäre beim Einsatz von People Analytics hin. Nicht angestrebt wird, einzelne People-Analytics-Anwendungen auf ihre rechtliche Zulässigkeit zu prüfen, da der Markt dieser Produkte viel zu gross dafür wäre.

Die vorliegende Abhandlung folgt einem chronologischen **Aufbau** vom Bewerbungsverfahren (II.A.) über das laufende Arbeitsverhältnis (II.B.) bis zur Beendigung desselben (II.C.). Die Zuordnung der zu besprechenden Fragekomplexe zum Bewerbungs-, Vertrags- oder Beendigungsstadium ist jedoch nicht zwingend. Z.B. kommen Eignungsabklärungen (dazu nachfolgend II.A.3.a) sowohl während der Anstellungsverhandlungen als auch im laufenden Arbeitsvertrag, etwa im Hinblick auf eine Beförderung, vor.³⁰ Ein Schlusswort bringt die erarbeiteten datenschutzrechtlichen Fragen am Ende auf den Punkt (III).

<<https://www.forbes.com/sites/joshbersin/2013/02/17/bigdata-in-human-resources-talent-analytics-comes-of-age/>> (besucht am 15.11.2018).

²⁷ Wie es die Autoren in ihrem SNF NFP 75-Projekt nennen, siehe FN 1.

²⁸ REINSCH/GOLTZ, 35.

²⁹ PORTMANN/RUDOLPH in BSK, Art. 328b OR N 48; PIETRUSZAK in KUKO, Art. 328 OR N 15; Gegebenenfalls können auch die DSGVO der Europäischen Union und nationale Gesetze der Mitgliedstaaten (Art. 88 DSGVO) auf Schweizer Arbeitsverhältnisse anwendbar sein: DAEDELLOW, 37.

³⁰ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 5.

II. People Analytics in den verschiedenen Phasen des Arbeitsverhältnisses

A. People Analytics in der Bewerbungsphase

1. Überblick über die relevanten Rechtsfragen

People Analytics beginnt bereits ganz am Anfang des Lebenszyklus eines Mitarbeiters, in der Phase der Rekrutierung und Personalauswahl (sog. Recruitment and Selection). Die verschiedenen Rechtsfragen zu People Analytics im Bewerbungsverfahren lassen sich für die vorliegenden Zwecke in **chronologischer Abfolge** darstellen: Zuerst stellt sich bei der Erstellung eines Wunschprofils die Frage nach der gültigen Einwilligung (II.A.2.), dann beim Vergleich und Aussortieren eingegangener Bewerbungen die Frage nach der zulässigen Eignungsabklärung (II.A.3.a) und schliesslich ist bei weitgehenden Erkundigungen über die Bewerber vor und während des Bewerbungsgesprächs zu beurteilen, inwieweit eine Persönlichkeitsdurchleuchtung zulässig ist (II.A.3.b).

2. Einwilligung der bestehenden Arbeitnehmer zur Erstellung eines Wunschprofils

Ausgangspunkt der Datenbearbeitung im Bewerbungsverfahren ist eine Analyse der bestehenden (erfolgreichen) Arbeitnehmer. Die Arbeitgeberin wertet nicht nur herkömmliche Datenpunkte, wie Ausbildung, Noten und Berufserfahrung, aus, sondern auch neue wie persönliche Performance³¹ oder das Verhalten in Computerspielen.³² Aus den verschiedenen Datensätzen kann sie Korrelationen ableiten, z.B. ist der regelmässige Besuch einer bestimmten japanischen Website für Manga-Comics angeblich ein verlässlicher Indikator für erstklassige Programmierer.³³ Gestützt darauf entwirft die Ar-

³¹ Z.B. Watson von IBM: F.A.Z.: Lieber Roboter als Personaler, Frankfurter Allgemeine Zeitung vom 01.03.2018, <<http://www.faz.net/aktuell/beruf-chance/beruf/bewer-berauswahl-durch-den-roboter-gar-nicht-so-abwegig-15473478.html>> (besucht am 05.07.2018).

³² KIM, 863.

³³ PECK DON: They're watching you at work, The Atlantic, <<https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/>>.

beitgeberin ein **Wunschprofil** (sog. Perfect Match), welches den Massstab für die Bewerber bildet.³⁴

Zunächst ist der Fall zu betrachten, in dem die Arbeitgeberin das Profil weniger Schlüsselmitarbeiter erstellt. Auch wenn sie die Daten anonymisiert, wird es häufig ohne unverhältnismässigen Aufwand möglich sein, von bestimmten Daten auf einen konkreten Arbeitnehmer zu folgern.³⁵ Es handelt sich dann um **Personendaten im Sinne des DSG** (Art. 3 lit. a). Das DSG ist somit anwendbar (Art. 1 DSG),³⁶ womit zu prüfen ist, ob ein Rechtfertigungsgrund für eine solche Datenbearbeitung besteht.³⁷

Die Arbeitgeberin darf Daten über den Arbeitnehmer nur bearbeiten, soweit diese dessen **Eignung** für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags **erforderlich** sind (Art. 328b Satz 1 OR). Die Analyse von Schlüsselmitarbeitern erfolgt nicht im Hinblick auf deren eigene Arbeitsverhältnisse, sondern zur Abklärung der Eignung von Bewerbern. Diese Begründung für die Datenerhebung ist somit untauglich.³⁸

Eine Persönlichkeitsverletzung infolge Datenbearbeitung ist nicht widerrechtlich, wenn sie durch ein **überwiegendes privates oder öffentliches Interesse** gerechtfertigt ist (Art. 13 Abs. 1 DSG). Die Arbeitgeberin hat ein vertretbares privates Interesse an einer geeigneten Selektion. Dem gegenüber steht das Interesse des Arbeitnehmers am Schutz seiner Privatsphäre. Die Sensitivität der Daten entscheidet über die Interessenabwägung.³⁹ Bei Daten über die Ausbildung und Qualifikation wird das Interesse der Arbeitgeberin überwiegen.⁴⁰ Hingegen überwiegt bei besonders schützenswerten Personendaten (Art. 3 lit. c DSG) in der Regel das Interesse des Arbeitnehmers. Zwischen diesen beiden Polen liegt eine grosse Grauzone.⁴¹ Die vorstehend genannten Daten zur persönlichen Performance fallen eher in die erste Kategorie, weil sie sich auf die Leistung am Arbeitsplatz beziehen und die Arbeit-

³⁴ BISSELS/MEYER-MICHAELIS/SCHILLER, 3043.

³⁵ DZIDA, 542.

³⁶ Eingehend zur Anwendbarkeit des DSG bei Re-Identifizierbarkeit nachfolgend, II.B.2.

³⁷ FLUECKIGER, Principes généraux, 7.

³⁸ DZIDA, 542.

³⁹ Ebd., 543.

⁴⁰ Ebd.

⁴¹ Ebd.

geberin sie ohnehin einsehen könnte. Tendenziell in die Letztere fallen Daten zum Game-Verhalten, da Computerspiele eine Freizeitaktivität darstellen und das Verhalten im Privatleben die Arbeitgeberin grundsätzlich nichts angeht. Das Erstellen von Korrelationen zwischen Freizeitgestaltungen und der Leistung am Arbeitsplatz ist somit rechtlich unzulässig, soweit die Arbeitgeberin kein überwiegendes Interesse an den entsprechenden Daten oder einen anderen Rechtfertigungsgrund vorweisen kann. Ein mögliches öffentliches Interesse an der Forschung im Bereich People Analytics kann den Eingriff in die Privatsphäre nicht generell rechtfertigen, zumal die Arbeitgeberin die erhobenen Daten nicht der Öffentlichkeit zur Verfügung zu stellen beabsichtigt.

Eine Persönlichkeitsprüfung infolge Datenbearbeitung könnte auch durch eine **Einwilligung** (Art. 13 Abs. 1 DSG) gerechtfertigt sein. Es ist umstritten, ob Arbeitnehmer gültig in eine Datenbearbeitung, die weder der Eignungsabklärung dient noch erforderlich ist, einwilligen können.⁴² Denn Art. 328b OR ist einseitig zwingend und die Parteien können nicht durch Abrede zuungunsten des Arbeitnehmers davon abweichen (Art. 362 Abs. 1 OR). Grund für diese relativ zwingende Geltung ist das jedem Arbeitsvertrag inhärente Abhängigkeitsverhältnis. Die Freiwilligkeit, die Voraussetzung für eine gültige Einwilligung ist, muss im Arbeitsbereich grundsätzlich äusserst kritisch betrachtet werden, da sich Arbeitnehmer aus verschiedenen Gründen unter Druck fühlen können.⁴³

Nach der wohl **herrschenden Meinung** soll eine Datenbearbeitung, die gegen Art. 328b OR verstösst, nur solange zulässig sein, als sie sich nicht zu Lasten des Arbeitnehmers auswirkt (Art. 362 Abs. 1 OR e contrario).⁴⁴ Die

⁴² Aufzählung der verschiedenen Lehrmeinungen in: PAPA/PIETRUSZAK, 17.7–17.8; PÄRLI, Datenaustausch, 159.

⁴³ EDÖB, Internet und E-Mailüberwachung, 5; MÉTILLE, 106.

⁴⁴ EDÖB, Personendaten, 6; STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 3; PORTMANN/RUDOLPH in BSK, Art. 328b OR N 26; PÄRLI, Datenaustausch, 159; FLUECKIGER, *Principes généraux*, 8–9; Pellascio in OFK, Art. 328b OR N 9; MÉTILLE, 106; HUGENTOBLE, 154; REHBINDER/Stöckli in BK, Art. 328b OR N 12; WINTERBERGER-YANG in BSK, Art. 328b/362 OR N 1; RIEMER-KAFKA, 290–291 präzisiert: Im Ergebnis sei es richtig, dass eine Einwilligung unter Verstoß gegen Art. 328b OR widerrechtlich sei. Die dogmatische Begründung sei aber nicht Art. 362 Abs. 1 OR, sondern dass die Einwilligung als einseitiges Rechtsgeschäft der Schranke von Art. 27 Abs. 2 ZGB unterliege.

Abweichung von Art. 328b OR muss für den Arbeitnehmer gesamthaft von Vorteil sein bzw. in dessen Interesse erfolgen.⁴⁵

Eine **liberalere Meinung** differenziert, dass es sich, obgleich relativ zwingendes Arbeitsrecht, um einen auf Arbeitsverhältnisse beschränkten Bearbeitungsgrundsatz (vgl. Art. 12 Abs. 2 lit. a DSG) handle. Art. 328b OR sei keine Verbotsnorm, deren Verletzung eine unerlaubte Handlung darstelle.⁴⁶ In den Gesetzesmaterialien⁴⁷ finde sich kein Hinweis, dass eine Verbotsnorm beabsichtigt worden sei.⁴⁸ Die Rechtfertigungsgründe des DSG (Art. 13 Abs. 1 DSG) könnten eine Verletzung von Art. 328b OR heilen:⁴⁹ Eine Einwilligung (Art. 13 Abs. 1 Variante 1 DSG) sei im Einzelfall möglich, wenn auch Art. 362 OR verbiete, zum Voraus auf den durch Art. 328b OR gewährten Schutz zu verzichten.⁵⁰ Demnach könne ein Arbeitnehmer gültig in die Speicherung von Daten über den Verlauf seiner privaten Internetnutzung einwilligen, indem er Internet-Guidelines unterschreibe.⁵¹ Ungültig wäre jedoch die Einwilligung, die der Arbeitgeberin zum Voraus ein umfassendes Recht einräumen würde, in beliebiger Weise in den privaten E-Mails des Arbeitnehmers zu stöbern.⁵² An die Einwilligung seien wegen des strukturellen Ungleichgewichts im Arbeitsverhältnis sehr hohe Anforderungen zu stellen,⁵³ umso mehr je ein-

⁴⁵ RAMPINI in BSK, Art. 13 DSG N 7.

⁴⁶ WILDHABER/HÄNSENBERGER, Internet, 317; PAPA/PIETRUSZAK, 17.8; MEIER, N 2037; ROSENTHAL in HKDSG, Art. 328b OR N 1, 5; Nach der DSGVO und dem deutschen Recht sei nicht von einer generellen Unzulässigkeit der Einwilligung auszugehen, KAINER/WEBER, 2742 und DZIDA, 543.

⁴⁷ Vgl. Botschaft zum Bundesgesetz über den Datenschutz vom 23.03.1988, BBl 1988 II, 413–534, 488.

⁴⁸ PAPA/PIETRUSZAK, 17.8 verweisen zudem auf Art. 18 Abs. 3 Satz 2 AVG, wonach eine Datenbearbeitung über Art. 328b OR hinaus mit Zustimmung des Arbeitnehmers erlaubt ist.

⁴⁹ ROSENTHAL in HKDSG, Art. 328b OR N 12; vgl. RIEMER-KAFKA, 287.

⁵⁰ PAPA/PIETRUSZAK, 17.8; MEIER, N 2040; vgl. RIESSELMANN-SAXER, 40.

⁵¹ WILDHABER/HÄNSENBERGER, Internet, 318; vgl. COSTA, N 17 FN 17, wonach im privaten Arbeitsbereich hauptsächlich die Einwilligung Rechtfertigungsgrund für die Internet- und E-Mail-Überwachung bilde; vgl. PÄRLI in SHK, Art. 328b OR N 27, wonach Personen, die sich auf eine leitende Funktion bewerben, bei hinreichender Transparenz ausdrücklich in die Durchleuchtung ihrer ganzen Persönlichkeit einwilligen können.

⁵² ROSENTHAL in HKDSG, Art. 328b OR N 14, 67.

⁵³ WILDHABER, 216.

schneidender der Eingriff in die Persönlichkeit des Arbeitnehmers⁵⁴ und je weiter die Datenbearbeitung vom Zweck der Durchführung des Arbeitsvertrags und der Eignungsabklärung (Art. 328b OR) entfernt sei.⁵⁵ Art. 27 Abs. 2 ZGB setze der gültigen Einwilligung enge Grenzen.⁵⁶ Das deutsche Recht⁵⁷ und die DSGVO⁵⁸ (E. 155: «auf der Grundlage einer Einwilligung») lassen eine Einwilligung zu, solange die konkreten Umstände im Einzelfall eine «echte und freie Wahl» (E. 42 DSGVO) zulassen. Hier ist zu gewichten, dass Schlüsselmitarbeiter insoweit eine stärkere und freiere Verhandlungsposition haben, als die Arbeitgeberin sie mehr als andere behalten will.

Konsequenterweise lässt die genannte liberalere Meinung, der wir hier folgen, neben der Einwilligung **auch die weiteren Rechtfertigungsmöglichkeiten** des DSG zu: Die Arbeitgeberin muss ihre gesetzlichen Verpflichtungen erfüllen können (vgl. Art. 13 Abs. 1 Variante 2 DSG; z.B. die Aufbewahrungspflichten nach Art. 958f OR und Art. 70 MWSTG), auch wenn damit eine Verletzung von Art. 328b OR einhergeht.⁵⁹ Es muss möglich bleiben, Daten über den in Art. 328b OR festgelegten Bearbeitungszweck hinaus zu bearbeiten, wenn ein überwiegendes privates⁶⁰ oder öffentliches⁶¹ Interesse besteht (vgl. Art. 13 Abs. 1 Variante 3 DSG).⁶² Es ist zulässig, dass die Arbeitgeberin Daten des Arbeitnehmers bearbeitet, die dieser allgemein zugänglich

⁵⁴ PAPA/PIETRUSZAK, 17.8.

⁵⁵ MEIER, N 2057.

⁵⁶ RIESSELMANN-SAXER, 37.

⁵⁷ Freiwillige Einwilligung möglich, selbst wenn eine Datenbearbeitung für den Arbeitnehmer nachteilig ist: DZIDA/GRAU, 189.

⁵⁸ Kritisch jedoch die Art.-29-Datenschutzgruppe, der zufolge die Einwilligung in der Regel «höchst unwahrscheinlich» als Rechtsgrundlage der Datenbearbeitung am Arbeitsplatz genüge, Art.-29-Datenschutzgruppe, Data processing, 3.

⁵⁹ PAPA/PIETRUSZAK, 17.8; SUBILIA/DUC, N 21; ROSENTHAL in HKDSG, Art. 328b OR N 12.

⁶⁰ Z.B. wenn die Arbeitgeberin einen Geschäftsbericht, in welchem der Mitarbeiter abgebildet ist, weiterhin Dritten zur Verfügung stellt, obwohl der Mitarbeiter das Unternehmen inzwischen verlassen hat; ebd.

⁶¹ Z.B. wenn die Arbeitgeberin Strafanzeige gegen einen Mitarbeiter erstattet, weil auf dessen Arbeitsplatzcomputer Kinderpornografie, die mutmasslich von ihm stammt, gefunden wird; ebd.

⁶² PAPA/PIETRUSZAK, 17.8; SUBILIA/DUC, N 20.

gemacht hat und deren Bearbeitung er nicht ausdrücklich untersagt (vgl. Art. 12 Abs. 3 DSGVO).⁶³

Aus dem Verbot der übermäßigen Selbstbindung (Art. 27 ZGB) folgt, dass der Arbeitnehmer seine Einwilligung jederzeit **widerrufen** kann.⁶⁴ Aus einem Widerruf dürfen ihm keine oder höchstens die Nachteile entstehen, die allein darin begründet sind, dass er die Vorteile des datenintensiveren Systems nicht nutzt.⁶⁵ Der Grundsatz von Treu und Glauben (Art. 2 Abs. 1 ZGB, vgl. Art. 4 Abs. 2 DSGVO) kann dem Widerrufsrecht jedoch Schranken setzen.⁶⁶ So können nach der bundesgerichtlichen Rechtsprechung Persönlichkeitsgüter, die nicht zum Kernbereich der menschlichen Existenz gehören, Gegenstand von vertraglichen und unwiderruflichen Verpflichtungen sein, wenn bei der fraglichen Verpflichtung wirtschaftliche Interessen im Vordergrund stehen.⁶⁷ Beispielsweise ist es möglich, Rechte am eigenen Bild, Namen oder der Stimme zum Zwecke der Vermarktung rechtlich verbindlich abzutreten, sodass ein Widerruf nicht mehr jederzeit und frei möglich ist.⁶⁸ Diese Rechtsprechung kommt zum Tragen, wenn wirtschaftliche Interessen des Arbeitnehmers an einer Abtretung bestehen. In dem Fall, in dem sich die Arbeitgeberin die Rechte an den Personendaten von Schlüsselmitarbeitern zum Zweck der Analyse dieser Schlüsselmitarbeiter abtreten lässt, stehen aber wirtschaftliche Interessen der Arbeitgeberin im Vordergrund, da sie aus der Analyse Vorteile ziehen will. Somit bleibt ein Widerruf der Einwilligung jederzeit und frei möglich.

Nach dem Gesagten erscheint die Einwilligung allein als fragiles Rechtfertigungsfundament,⁶⁹ weil einerseits ihre Zulässigkeit umstritten ist, wenn die Datenbearbeitung zum Nachteil des Arbeitnehmers erfolgt, und andererseits jederzeit ein Widerruf droht. Die Arbeitgeberin sollte ihre **Restrisiken** minimieren, indem sie die Bedingungen der Datenbearbeitung vor

⁶³ PAPA/PIETRUSZAK, 17.8.

⁶⁴ RAMPINI in BSK, Art. 13 DSGVO N 14.

⁶⁵ HOFMANN, 14, mit Bezug auf das deutsche und europäische Recht.

⁶⁶ Zur deutschen Rechtsprechung: DZIDA/GRAU, 190; DZIDA, 543.

⁶⁷ BGE 136 III 401 E. 5.2.2.

⁶⁸ Ebd.

⁶⁹ BISSELS/MEYER-MICHAELIS/SCHILLER, 3045.

dem Einholen der Einwilligung transparent kommuniziert und über einen sorgfältigen Umgang mit den Daten das Vertrauen der Mitarbeiter gewinnt.

Als Ausweg bleibt der Arbeitgeberin, **Daten von vielen** (allenfalls nicht mehr nur Schlüssel-)Mitarbeitern auszuwerten, sodass eine Identifizierung konkreter Personen nicht mehr oder nur mit unverhältnismässigem Aufwand möglich ist bzw. die Daten anonymisiert bleiben.⁷⁰ Die Datenbearbeitung unterliegt dann nicht dem DSG (Art. 1 i.V.m. Art. 3 lit. a DSG e contrario).⁷¹ Dehnt die Arbeitgeberin ihren Datensatz dergestalt aus, sinkt auch ihr Schadensrisiko, falls einzelne Arbeitnehmer ihre Einwilligung doch widerrufen sollten.

Zwischenfazit: Die Analyse der Schlüsselmitarbeiter zum Zweck der Selektion kann in vielen Fällen erfolgreich angefochten werden. Die Datenbearbeitung kann in Bezug auf Daten gerechtfertigt sein, an welchen die Arbeitgeberin überwiegende Interessen vorweisen kann. Eine Einwilligung sollte nicht alleinigen Rechtfertigungsgrund bilden.

3. Bearbeitung der Daten der Bewerber

a) Eignungsabklärung anhand der vom Bewerber mitgeteilten Informationen

Nachdem das Wunschprofil erstellt ist, vergleicht ein Algorithmus es mit den eingegangenen Bewerbungen und sortiert gegebenenfalls erste Bewerbungen aus (sog. **Short-Listing**, Hiring by Algorithm oder E-Recruiting). Rund jedes zwanzigste (5,1 %) schweizerische Grossunternehmen verwendet ein

⁷⁰ DZIDA, 543.

⁷¹ Siehe aber zur Anwendbarkeit des DSG bei potentieller Re-Individualisierung nachfolgend II.B.2.

solches Short-Listing-Verfahren.⁷² Vergleichbar ist die Lage in Deutschland (Anwendung bei 6 % der deutschen Grossunternehmen).⁷³

Für den algorithmen-basierten Vergleich der eingegangenen Bewerbungen mit dem vordefinierten Profil beruft sich die Arbeitgeberin auf den Rechtfertigungsgrund der **Eignungsabklärung** (1. Variante von Art. 328b Satz 1 OR). Nicht in Frage kommt bei der Analyse von Bewerbern die Berufung auf die Erforderlichkeit (2. Variante von Art. 328b Satz 1 OR), da diese nur die Zeit während einer Anstellung betrifft.⁷⁴ Die Daten müssen objektiv zur Abklärung der hinreichenden Eignung im Hinblick auf eine konkrete Stelle beitragen.⁷⁵ Nicht entscheidend ist die subjektive Wissbegier der Arbeitgeberin.⁷⁶

Sowohl die persönliche als auch die fachliche bzw. **berufliche Qualifikation** geben objektiv Aufschluss über die hinreichende Befähigung.⁷⁷ Angaben zur beruflichen Qualifikation umfassen namentlich Aus- und Weiterbildung, Berufserfahrung, Sprachkenntnisse, Auslandsaufenthalte und berufliche Pläne.⁷⁸ Die Belastbarkeit, Kommunikationsfähigkeit, Teamfähigkeit gehören unseres Erachtens ebenfalls zur beruflichen Qualifikation. Denn diese Fähigkeiten werden schon in der Primarschule benotet und sind zentral im Berufsleben, besonders in der Zukunft. Teilweise werden sie als Elemente der persönlichen Qualifikation eingestuft.⁷⁹ Der Bewerber macht die Angaben (z.B. zur schulischen Note) in der Regel, um der Arbeitgeberin zu zeigen, dass er ihre Erwar-

⁷² In der Studie der Autoren (siehe FN 1 und 21) nahmen 158 schweizerische Grossunternehmen 2018 an einer Online-Umfrage teil. 5,1 % der Teilnehmenden gaben an, technologiebasiertes Short-Listing zur Vorselektion anzuwenden, um den Bewerbungsprozess effizienter zu gestalten. Ebenfalls 5,1 % der Teilnehmenden gaben an, mit technologischer Unterstützung die für eine Stelle erforderlichen Kompetenzen mit den Fähigkeiten der Arbeitnehmer abzugleichen, um die am besten geeigneten Kandidaten anzustellen. Bereits seit Längerem ist der Einsatz von Hiring by Algorithm bei Swiss, Manor, IBM oder der Berner Kantonsverwaltung bekannt: WILDHABER, 214.

⁷³ F.A.Z.: Lieber Roboter als Personaler, Frankfurter Allgemeine Zeitung vom 01.03.2018, <<http://www.faz.net/aktuell/beruf-chance/beruf/bewerbersauswahl-durch-den-roboter-gar-nicht-so-abwegig-15473478.html>> (besucht am 05.07.2018).

⁷⁴ EDÖB, Personendaten, 6.

⁷⁵ WILDHABER/HÄNSENBERGER, Internet, 327; STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 5.

⁷⁶ PIETRUSZAK in KUKO, Art. 328b OR N 6.

⁷⁷ Ebd.

⁷⁸ Ebd.; REHBINDER/Stöckli in BK, Art. 328b OR N 5; EMMEL in CHK, Art. 328b OR N 4.

⁷⁹ Ebd.; STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 5; ARYANI, 1073.

tungen erfüllt und sich im Vergleich zu anderen Bewerbern abzuheben. Dass ein Algorithmus die Angaben mit dem Wunschprofil der Arbeitgeberin vergleicht, erscheint vom Zweck, zu dem die Daten bekanntgegeben wurden, abgedeckt. Die Arbeitgeberin hat bei sehr vielen Bewerbungen ein vertretbares Interesse daran, ihren Aufwand zu reduzieren, indem sie etwa den Notenvergleich automatisiert.

Zur **persönlichen Qualifikation** gehören z.B. Charakter, Weltanschauung⁸⁰, und Freizeitgestaltung.⁸¹ Grundsätzlich unzulässig ist die Abklärung persönlicher Verhältnisse und Eigenschaften, die nicht wesentlich die beruflichen Fähigkeiten mitbestimmen.⁸² Je höher jedoch die Stellung im Betrieb ist, desto umfassender darf die Abklärung ausfallen.⁸³ Für Stellen mit sehr grosser Verantwortung und hohen Anforderungen an die persönliche Integrität sind vertiefte Abklärungen wegen Haftungs- und Reputationsrisiken sogar geboten.⁸⁴ Tendenzbetriebe dürfen in Bezug auf ihren ideellen Zweck Daten aus dem Privatbereich bearbeiten, die keinen engen Bezug zur betreffenden Arbeit aufweisen, sofern der Arbeitnehmer Tendenzträger ist.⁸⁵ Bei vorwiegend ausführenden Tätigkeiten muss sich die Datenbearbeitung auch bei Tendenzbetrieben auf die berufliche Qualifikation beschränken.⁸⁶

Die Technologie ermöglicht den Einbezug **neuer Kriterien**, die bislang nicht zur Beurteilung der Eignung beigetragen haben. Eine Big-Data-Analyse kann eine Korrelation zwischen irgendeiner Freizeitgestaltung und der Arbeit hervorbringen (z.B., wie vorstehend unter II.A.2. beschrieben, zwischen dem Verhalten in Computerspielen und der überdurchschnittlichen Leistung). Es besteht Klärungsbedarf hinsichtlich der Frage, was objektiv zur Eignungsabklärung hilft. In die Beantwortung dieser Frage müssen die Eckdaten der jeweils zu besetzenden Stelle einfließen. Grundsätzlich zulässig erscheint die Bearbeitung von Daten, die der Bewerber unaufgefordert mitteilt (z.B. ein Lebenslauf mit Angaben zur persönlichen Qualifikation, welche für die kon-

⁸⁰ PIETRUSZAK in KUKO, Art. 328b OR N 6.

⁸¹ BAUMANN, 640.

⁸² EDÖB, Personendaten.

⁸³ EMMEL in CHK, Art. 328b OR N 2.

⁸⁴ PÄRLI in SHK, Art. 328b OR N 27.

⁸⁵ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 5; PELLASCIO in OFK, Art. 328b OR N 7.

⁸⁶ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 5.

krete Stelle nicht relevant sind), weil dann von der Einwilligung des Bewerbers auszugehen ist.⁸⁷ Dagegen ist es problematisch, wenn die Arbeitgeberin solche Angaben zusätzlich zu den freiwillig eingereichten verlangt (z.B. wenn sie das Spielen eines Videogames als Teil eines Bewerbungsprozesses vorschreibt und dabei das Spielverhalten beobachtet). Es kann nicht ohne Weiteres von einer rechtfertigenden, freiwilligen Einwilligung ausgegangen werden, da sich ein Stellenbewerber gezwungen fühlt, die Daten zu übermitteln, um die Stelle zu erhalten. Hier muss die Arbeitgeberin erklären können, inwiefern die Daten objektiv der Eignungsabklärung dienen.

Sortiert der Algorithmus, und nicht ein Mensch, unpassende Bewerbungen direkt aus, sind gegebenenfalls die Bestimmungen zu **automatisierten Einzelfallentscheiden** zu prüfen.⁸⁸ Während das geltende DSG diesen Begriff nicht kennt,⁸⁹ ist eine solche Regelung künftig geplant (Art. 19 E-DSG) und findet im Geltungsbereich der DSGVO bereits Anwendung (Art. 22 DSGVO).

Zwischenfazit: Der algorithmische Vergleich von Daten aus Bewerbungsunterlagen mit dem Wunschprofil erscheint grundsätzlich zulässig, solange die Bewerber ihre Daten freiwillig mitgeteilt haben. Haben die Bewerber die Daten jedoch aus einer Zwangslage heraus mitgeteilt, muss die Arbeitgeberin erklären können, inwiefern die Daten objektiv der Eignungsabklärung dienen. Klärungsbedarf besteht bei der Frage, was alles noch als objektives Kriterium zur Eignungsabklärung in Bezug auf eine konkrete Stelle zählen kann. Diese Klärung wird mit der fortschreitenden Technologie zunehmend drängender, weil die Algorithmen immer neue Korrelationen aufdecken und Kriterien festmachen werden, die heute nicht als Kriterien für die Beurteilung der Eignung bekannt sind. Versteht sich «objektiv» als sachlich nachvollziehbar, so kann eine bloße Korrelation noch kein genügend objektives Kriterium für die Eignungsabklärung sein. Kann die Arbeitgeberin hingegen eine Kausalität zwischen einer Eigenschaft des Bewerbers und der Eignung für eine Stelle nachweisen, so ist die sachliche Nachvollziehbarkeit gegeben.

⁸⁷ Vgl. ROSENTHAL in HKDSG, Art. 328b OR N 12.

⁸⁸ Dazu WILDHABER, 216–217.

⁸⁹ Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017, 6941–7192, 7056.

b) Persönlichkeitsdurchleuchtung anhand der durch die Arbeitgeberin erforschten Informationen

Nach dem ersten Vergleich und Aussortieren der Bewerbungen holt die Arbeitgeberin zusätzliche Informationen ein:

- Ein **Algorithmus zur Internetrecherche** sammelt Millionen im Internet auffindbarer Datenpunkte über die verbleibenden Bewerbungen, z.B. frühere Arbeitsleistungen, Ausbildung, gesellschaftliche Vorlieben, bevorzugter Browser, Reiseziele oder Sprache,⁹⁰ ebenso, welche Websites die Person besucht, positive oder negative Art der Sprache, mit der die Person Technologien beschreibt, auf LinkedIn selbst angegebene Fähigkeiten⁹¹ oder, wie die arbeitsrelevanten Beiträge der Bewerber in Online-Foren von anderen bewertet werden.⁹² Diese Informationen sind wohl mehrheitlich im oberflächlichen, von den gewöhnlichen Suchmaschinen indexierten Teil des Internets (sog. Surface Web) auffindbar. Angeboten werden jedoch auch sog. **Deep Web Crawlers**.⁹³ Diese «Kriechtiere» schlängeln sich durch den von gewöhnlichen Suchmaschinen nicht indexierten (weil z.B. Login-geschützten) Teil des World Wide Web (sog. Deep Web).
- In Zeiten des Fachkräftemangels ist es möglicherweise keine Option, sich mit den eingegangenen Bewerbungen zu begnügen. Stattdessen sucht ein Algorithmus im Internet für die Arbeitgeberin laufend aktiv nach geeigneten Kandidaten, die trotz bestehenden Arbeitsvertrags mit einem Drittunternehmen latent zu einem Stellenwechsel bereit wären (sog. **Active Sourcing**⁹⁴). Anzeichen für eine Wechselbereitschaft bestehen, wenn eine Person nach längerer Zeit ihr Profil in den sozialen Netzwerken auf

⁹⁰ SNYDER, 243.

⁹¹ Z.B. die Funktion Smart Hiring Platform von Gild: KIM, 862.

⁹² Z.B. Remarkable Hire: REINSCH/GOLTZ, 37.

⁹³ Z.B. von Spokeo: SNYDER, 275; Spokeo beschränkt sich nach eigenen Angaben auf die Durchsuchung der öffentlichen Teile des Deep Web, Spokeo: The deep web vs. the dark web: What's the difference?, 06.11.2017, <<https://www.spokeo.com/compass/difference-between-deep-web-and-dark-web/>> (besucht am 31.08.2018).

⁹⁴ KAINER/WEBER, 2743; angeboten z.B. von Entelo (REINSCH/GOLTZ, 37), Joberate oder Talentwunder (Braehmer: Ab wann werden viele Daten im Personalwesen HR-Big-Data?, 12.08.2016, <<https://intercessio.de/ab-wann-werden-viele-daten-im-personalwesen-big-data/>> (besucht am 05.02.2018)).

den neusten Stand bringt, oder je nachdem, welche ihr zugesandten Inhalte sie liest und welche nicht.⁹⁵

- Lädt die Arbeitgeberin zum **Bewerbungsgespräch**, verlässt sie sich auf die Unterstützung einer Software zur Spracherkennung und Analyse, ob die passiven Verhaltenscharakteristiken des Bewerbers zur Stelle passen.⁹⁶ Roboter können zum Einsatz kommen (sog. Hireobotics Solutions), um Bewerber zu befragen, auf Fragen zu antworten und die physiologischen Reaktionen (z.B. Herzschlag, Augenbewegungen, Gesichtsausdruck) eines Bewerbers zu messen.⁹⁷ Alle diese (angeblich) objektiven Datenaufzeichnungen sollen im Interesse der Bewerber die subjektiven Eindrücke und Vorurteile der Arbeitgeberin relativieren⁹⁸ und die Diversität in der Belegschaft fördern.⁹⁹

Technisch möglich ist eine regelrechte **Durchleuchtung der Persönlichkeit** des Bewerbers. Bei den geschilderten Anwendungen kann der Algorithmus die Persönlichkeit verletzen, indem er Daten aufspürt, die der Bewerber nicht zum Zweck einer solchen Analyse freigegeben hat (vgl. Art. 12 Abs. 3 i.V.m. Art. 4 Abs. 3 DSGVO). Von den erhobenen Daten kann ein Algorithmus auf weitere Eigenschaften einer Person schliessen (z.B. von Körpergrösse und -gewicht auf das Geschlecht, von der Postleitzahl auf die Ethnie oder vom Essen auf die Religion).¹⁰⁰ Auch eine Prognose zum künftigen Verhalten des Bewerbers ist möglich: Voraussagende Analysen (sog. Predictive Analytics) arbeiten mit Modellen, die anhand von Daten der Gegenwart und Vergangenheit die Zukunft voraussagen.¹⁰¹ Dies ermöglicht z.B., eine latente Bereitschaft zu einem Jobwechsel aufzudecken. Dabei ist die wissenschaftliche Verlässlichkeit von Big-Data-Analysen umstritten, weil es sich um eine induk-

⁹⁵ So die Personaldienstleister Hays und Manpower: GRATWOHL: Wie Personalvermittler auf LinkedIn und Xing nach Talenten suchen, Neue Zürcher Zeitung vom 08.01.2018, <<https://www.nzz.ch/wirtschaft/raffinierte-jagd-auf-talente-ld.1345229>> (besucht am 26.11.2018).

⁹⁶ Z.B. HireIQ und Infor Talent Science: SNYDER, 253.

⁹⁷ Z.B. der Roboter Sophie: WILDHABER, 216.

⁹⁸ So Cognissess Deep Learn: vgl.: Calling on his people skills, The Bath Chronicle vom 13.10.2016, 38–39.

⁹⁹ So Textio: KIM, 872.

¹⁰⁰ SNYDER, 257.

¹⁰¹ Ebd., 250.

tive und untheoretische Suche nach beliebigen statistischen Korrelationen handelt.¹⁰² Untheoretisch bedeutet, dass eine Theorie fehlt bzw. nicht im Voraus der Analyse bekannt ist, wonach gesucht wird. Das Schürfen nach Daten (sog. Data Mining) kann zwar dazu dienen, vermutete Beziehungen zu bestätigen (sog. Top-down- oder theoriegetriebener Ansatz), aber ebenso dazu, unbekannte Muster zu entdecken (sog. Bottom-up- oder datengetriebener Ansatz).¹⁰³ Im letzteren Fall stützen sich die Praktiken des Personalwesens nicht mehr auf eine geprüfte Theorie mit kausalen Annahmen, sondern auf auffällige Korrelationen in einem Meer an Daten. Eine theoretische Erklärung dafür, dass die Korrelationen auch Kausalitäten sind, fehlt. Personalmanagement wird durch Big Data zwar empirischer und stärker datengetrieben, aber nicht notwendigerweise theoretisch fundierter.¹⁰⁴

Genauso umstritten wie Big-Data-Analysen ist der wissenschaftliche Wert von **graphologischen Gutachten** handgeschriebener Lebensläufe und psychologischer Eignungstests.¹⁰⁵ Deshalb ist ein Blick auf die Nutzung graphologischer Gutachten im Bewerbungsprozess aus rechtlicher Perspektive hilfreich. Mitte der 90er-Jahre holten rund zwei Drittel (68 %) der Unternehmen bei der Auswahl von Führungskräften regelmässig graphologische Gutachten über die Bewerber ein.¹⁰⁶ Auch noch 2011 waren graphologische Gutachten in der Schweiz verbreitet.¹⁰⁷ Sie müssen kumulativ die folgenden rechtlichen Voraussetzungen erfüllen:

- Die vorgängige ausdrückliche **Einwilligung** des Bewerbers ist erforderlich (vgl. Art. 4 Abs. 5 Satz 2 DSG).¹⁰⁸ Die Zustimmung kann konkludent erfolgen, z.B. wenn die Arbeitgeberin den handgeschriebenen Lebenslauf zur Anfertigung eines graphologischen Gutachtens fordert und der Bewerber

¹⁰² KIM, 879–880.

¹⁰³ CUSTERS *et al.*, 9.

¹⁰⁴ KAISER, 14.

¹⁰⁵ REHBINDER/STÖCKLI in BK, Art. 320 OR N 6.

¹⁰⁶ ZÜST, 1476.

¹⁰⁷ Z.B. bei Implenia, Miele, Netstal, dem VCS und der Stadt Zürich: STEIGER: Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, <<https://steigerlegal.ch/2011/10/21/schweizerische-arbeitgeber-auf-graphologischen-abwegen/>> (besucht am 29.08.2018).

¹⁰⁸ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 10.

ihn kommentarlos schickt.¹⁰⁹ Das Einreichen einer Schriftprobe allein stellt hingegen keine Einwilligung dar.¹¹⁰ Ziel des Gutachtens und der Zusammenhang zur ausgeschriebenen Stelle müssen klar sein (vgl. Art. 4 Abs. 5 Satz 1 DSG).¹¹¹ Es darf nicht ein zu anderen Zwecken handschriftlich verfasster Text verwendet werden (vgl. Art. 4 Abs. 3 DSG).¹¹² Die Einwilligung muss freiwillig erfolgen (Art. 4 Abs. 5 Satz 1 DSG).

- Das graphologische Gutachten muss sich auf die **Arbeitsplatzzeignung** beschränken.¹¹³ Das Durchleuchten der ganzen Persönlichkeit ist zwar möglich, die ausdrückliche Einwilligung ist aber vorausgesetzt.¹¹⁴ Allgemeine Charakterstudien sind unzulässig.¹¹⁵
- Nachvollziehbare, zuverlässige und **objektive Ergebnisse** müssen resultieren. Die Methoden müssen fachmännisch angewendet und ausgewertet werden.¹¹⁶

Die Voraussetzungen für graphologische Gutachten lassen sich auf Anwendungen von People Analytics, welche die Persönlichkeit des Bewerbers durchleuchten, **in vergleichbarer Weise** übertragen: Eine vorgängige Einwilligung ist erforderlich. Eine konkludente Einwilligung liegt z.B. vor, wenn die Arbeitgeberin die Einreichung der Dissertation in Wordformat zum Zweck einer Persönlichkeitsanalyse fordert und der Bewerber das Word-Dokument kommentarlos schickt.¹¹⁷ Welche neuen Kriterien objektiv etwas über die Arbeitsplatzzeignung aussagen, ist weitgehend unerforscht (dazu vorstehend II.A.3.a). Problematisch erscheint etwa die Ermittlung, ob ein Bewerber seiner Persönlichkeit nach generell zu Straftaten neigt.¹¹⁸

Die Grenze zwischen einer Persönlichkeitsdurchleuchtung und dem, was diese Schwelle nicht erreicht, ist fließend. **Keine Durchleuchtung der Per-**

¹⁰⁹ DZIDA, 544.

¹¹⁰ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 10.

¹¹¹ STEIGER, FN 107; HUGENTOBLE, 154.

¹¹² STEIGER, FN 107.

¹¹³ Ebd.

¹¹⁴ PÄRLI in SHK, Art. 328b OR N 27.

¹¹⁵ REHBINDER/STÖCKLI in BK, Art. 320 OR N 6; STEIGER, FN 107.

¹¹⁶ Ebd.

¹¹⁷ DZIDA, 544.

¹¹⁸ Ebd., 545.

sönlichkeit liegt vor, wenn sowohl die bearbeiteten Daten als auch die gezogene Schlussfolgerung vom Kern des Persönlichkeitsrechts sehr weit entfernt liegen.¹¹⁹ Entscheidend ist ein objektiver Massstab.¹²⁰ Es stellt noch keine unzulässige Persönlichkeitsdurchleuchtung dar, wenn die Arbeitgeberin künftiges Verhalten über das einem traditionellen Vorgesetzten mögliche Mass hinaus prognostizieren kann.¹²¹ Äussert eine Person im öffentlich zugänglichen Teil eines sozialen Netzwerks Absichten über einen Stellenwechsel, kann der Algorithmus eine entsprechende Verhaltensprognose erstellen, während ein traditioneller Personalverantwortlicher keine Zeit für Diagnosen sozialer Netzwerke haben mag. Gleichwohl handelt es sich noch nicht um eine Ergründung der Persönlichkeit.¹²² Ebenfalls keine Persönlichkeitsdurchleuchtung liegt vor beim Einsatz einer Plagiatsoftware zur Überprüfung der online jedermann zugänglichen Dissertation daraufhin, ob der Verfasser den in der Bewerbung angegebenen akademischen Grad auf rechtmässigem Weg erlangt hat. Eine solche Analyse auf Plagiate hin ist zur Eignungsabklärung zulässig.¹²³

Zu ergänzen ist, dass sich People Analytics selbstverständlich an die Grenzen des **Strafrechts** halten muss. Das Eindringen in die geschützten Kammern des World Wide Web mit einem Deep Web Crawler kann gegen Bestimmungen des Strafgesetzbuchs verstossen (insbesondere Art. 179 ff. StGB).

Zwischenfazit: People Analytics kann zur Analyse der Persönlichkeit eines Bewerbers eingesetzt werden. People Analytics ist in solchen Fällen mit herkömmlichen Techniken zur Persönlichkeitsanalyse, wie z.B. den graphologischen Gutachten, vergleichbar. Stimmt man diesem Vergleich zu, gelten die Voraussetzungen der Einwilligung, Eignungsabklärung und objektiven Ergebnisse. Über die rechtlichen Probleme zur Einwilligung und Eignungsabklärung wurde vorstehend (II.A.2.) und II.A.3.a) berichtet. Die Objektivität der mit statistischen Korrelationen gewonnenen Ergebnisse zur Persönlichkeit ist ausserdem fraglich. An eine Persönlichkeitsdurchleuchtung mit Hilfe von People Analytics sind daher hohe rechtliche Anforderungen zu stellen.

¹¹⁹ Vgl. DZIDA, 545.

¹²⁰ Vgl. WOLFER, N 183–184.

¹²¹ DZIDA, 545.

¹²² Ebd.

¹²³ Ebd., 544.

c) Frageverbot

Aus Art. 328b OR resultiert ein **Frageverbot** der Arbeitgeberin in Bezug auf die Privatsphäre des Arbeitnehmers.¹²⁴ Unzulässig sind etwa Fragen nach Schwangerschaft(sabsichten), Rauchgewohnheiten,¹²⁵ Herkunft, Gewerkschaftszugehörigkeit, religiöser oder politischer Gesinnung, es sei denn, das Unternehmen habe eine entsprechende ideelle Zielsetzung.¹²⁶ Den Bewerbern steht im Fall einer unzulässigen Frage ein Notwehrrecht auf Lüge zu.¹²⁷

Bewerber erlangen keine Kenntnis davon, dass ein Algorithmus im Internet Daten über sie aufspürt. Ihr Notwehrrecht zur Lüge können sie faktisch nicht ausüben. Somit muss die Arbeitgeberin den Algorithmus so **programmieren**, dass er von sich aus keine Daten zur Privatsphäre ermittelt. Er darf z.B. nicht prüfen, ob sich die Bewerberin in sozialen Netzwerken äussert, in denen es um Schwangerschaftsthemen geht.¹²⁸

d) Diskriminierungsverbot

In der Schweiz fehlt ein Erlass zum umfassenden arbeitsrechtlichen Verbot von Diskriminierungen, wie er etwa in Deutschland mit dem Allgemeinen Gleichbehandlungsgesetz (AGG) existiert. Die Schweiz kennt bloss partielle Diskriminierungsbestimmungen, die die Merkmale Geschlecht (GlG), Behinderung (BehiG), genetische Abstammung (GUMG), Staatsangehörigkeit (FZA), und auch Alter (Art. 328, Art. 336 Abs. 1 lit. a OR)¹²⁹ schützen. Eine Ungleichbehandlung aufgrund diskriminierungssensibler Merkmale stellt aber eine Verletzung der Arbeitnehmerpersönlichkeit dar. Somit ist der Diskriminierungsschutz über den **allgemeinen Persönlichkeitsschutz** zu verwirklichen, der nicht (nur) bestimmte gesellschaftliche Gruppen vor Diskrimi-

¹²⁴ FLUECKIGER, Googleisation, 78.

¹²⁵ KAINER/WEBER, 2742.

¹²⁶ EDÖB, Personendaten, 9.

¹²⁷ PÄRLI in SHK, Art. 328b OR N 36. Das Bundesgericht erwähnt das Notwehrrecht der Lüge in BGE 122 V 267 E. 4c. Wenn die Arbeitgeberin Dokumente verlangt, soll der Bewerber nach deutschem Recht ein Recht zur Fälschung haben, KAINER/WEBER, 2742.

¹²⁸ DZIDA, 543.

¹²⁹ EMMEL in CHK, Art. 328 OR N 6.

nierung schützt.¹³⁰ Der allgemeine Gleichbehandlungsgrundsatz in der Gestalt des individuellen Diskriminierungsverbots¹³¹ verbietet willkürliche Entscheidungen der Arbeitgeberin, in denen eine den Arbeitnehmer verletzende Geringschätzung seiner Persönlichkeit zum Ausdruck kommt. Eine solche Geringschätzung kann nur bestehen, wenn ein Arbeitnehmer gegenüber einer Vielzahl von anderen Arbeitnehmern deutlich ungünstiger gestellt wird, ohne dass hierfür sachliche Gründe vorliegen. Keine solche Geringschätzung ist gegeben, wenn die Arbeitgeberin bloss einzelne Arbeitnehmer besser stellt.¹³²

Algorithmen, die im Bewerbungsverfahren zum Einsatz kommen, müssen so **programmiert** sein, dass sie Schutz vor direkter und indirekter Diskriminierung bieten.¹³³ Dabei ist zu beachten, dass Daten stellvertretend als Angabe über die Zugehörigkeit eines Arbeitnehmers zu einer geschützten Gruppe stehen können.¹³⁴ Relativ triviale Informationen können eng mit geschützten Charakteristika korrelieren (z.B. Facebook-Likes mit Geschlecht oder politischer Gesinnung).¹³⁵ Das schweizerische Diskriminierungsverbot vermag deshalb nicht zu genügen, zumal es an Beweisschwierigkeiten leidet und es kaum abschreckende Sanktionen gibt.¹³⁶

B. People Analytics während des laufenden Arbeitsvertrags

1. Überblick über die relevanten Rechtsfragen

Die Arbeitgeberin kann People Analytics **zu allen erdenklichen Zwecken** während des laufenden Arbeitsvertrags verwenden. Einsatzgelegenheiten bieten sich etwa in den Bereichen Leistungssteuerung (sog. Performance

¹³⁰ Hierzu der Vortrag der Autorin «Diskriminierung durch Big Data in der Arbeitswelt – Rechtliche Überlegungen» anlässlich des Law & Robots-Workshops vom 16.05.2018 an der Universität Basel.

¹³¹ EMMEL in CHK, Art. 328 OR N 6.

¹³² BGE 129 III 276 = BGer 4C.269/2002 E. 3.1.

¹³³ WILDHABER, 214.

¹³⁴ WILSON/BELLIVEAU/GRAY, 33.

¹³⁵ KIM/HANSON, 19.

¹³⁶ WILDHABER, Roboter, 337.

Management), Compliance Management, Mitarbeiterbindung und Personalwechsel (sog. Retention and Transition) sowie die Arbeits- und Arbeitsplatzgestaltung (sog. Work and Workplace Design). Diese Anwendungen folgen einander nicht chronologisch, sondern können alle gleichzeitig zum Einsatz kommen.

Das vorliegende Kapitel kann nur ausgewählte Beispiele der vielfältigen Palette von People Analytics vorstellen. Statt Anwendungen einzeln durchzugehen, konzentrieren wir uns auf die folgenden drei **datenschutz- und gesundheitsschutzrechtlichen Fragen**, die zur Prüfung der rechtlichen Zulässigkeit aller People-Analytics-Systeme wichtig erscheinen: Abgrenzung Personen- und Sachdaten bzw. sachlicher Anwendungsbereich des DSGVO (nachfolgend 2), Abgrenzung privater von allgemein zugänglichen Personendaten (nachfolgend 3) sowie Verhaltensüberwachung am Arbeitsplatz (nachfolgend 4).

2. Abgrenzung Personen- und Sachdaten

Das DSGVO ist sachlich anwendbar auf die Bearbeitung von **Personendaten** (Art. 1 DSGVO). Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSGVO).

Bestimmtheit einer Person bedeutet, dass sich direkt aus der Information selbst ergibt, dass es sich genau um diese Person handelt.¹³⁷ Dies ist z. B. bei einem Personalausweis der Fall.¹³⁸

Bestimmbar ist eine Person, wenn indirekt aufgrund einer Kombination verschiedener Informationen auf sie geschlossen werden kann (z.B. aufgrund von Sachen, die einer Person gehören).¹³⁹ Massgebend für die Bestimmbarkeit ist der objektiv erforderliche Aufwand (z.B. Kosten, Zeitaufwand), um eine bestimmte Information einer Person zuordnen zu können. Es genügt nicht jede theoretische Möglichkeit der Identifizierung; ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ihn ein Interessent auf sich nehmen wird, liegt keine Be-

¹³⁷ PORTMANN/RUDOLPH in BSK, Art. 328b OR N 3; REHBINDER/Stöckli in BK, Art. 328b OR N 2; BAERISWYL, 49.

¹³⁸ Botschaft zum Bundesgesetz über den Datenschutz vom 23.03.1988, BBl 1988 II, 413–534, 444.

¹³⁹ BAERISWYL, 49; REHBINDER/Stöckli in BK, Art. 328b OR N 2.

stimmbarkeit vor. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind.¹⁴⁰

Sachdaten sind demgegenüber kein Schutzobjekt des DSG, d.h. sie unterstehen dem Gesetz nicht. Sie weisen keinen Personenbezug auf und er lässt sich auch nicht herstellen.¹⁴¹ Hierzu zählen auch statistische und anonymisierte Personendaten, sofern die Anonymisierung irreversibel ist.¹⁴² Die einfache Namensänderung eines Arbeitnehmers genügt nicht als Anonymisierung.¹⁴³

Bei People Analytics wird es immer schwieriger¹⁴⁴ und ergibt es immer weniger Sinn,¹⁴⁵ Personen- und Sachdaten auseinanderzuhalten. Mit den verwendeten Big-Data-Techniken kann die Arbeitgeberin bereits von wenigen anonymisierten Daten Personen **re-identifizieren**.¹⁴⁶ Zu betrachten ist etwa der Fall, wenn für die Identifizierung einer Person die «komplizierte Analyse einer Statistik» erforderlich wäre: Während hier aus Sicht des Bundesrats 1988 die Bestimmbarkeit fehlte,¹⁴⁷ ist eine Re-Identifizierung vor dem Hintergrund von Big Data heute in vielen Fällen möglich geworden.¹⁴⁸

Bei reinem Abstellen auf die technische Möglichkeit der Re-Identifizierung würden (künftig) fast alle People-Analytics-Anwendungen unter das DSG fallen, weil der objektive Aufwand der Bestimmbarkeit mit Big Data stetig abnimmt. Die bundesgerichtliche Rechtsprechung fordert im Leitentscheid BGE 136 II 508 für die Annahme der Bestimmbarkeit jedoch zusätzlich, dass die Datenbearbeiterin **ein (subjektives) Interesse** daran hat, den für eine Identifizierung nötigen Aufwand zu betreiben (sog. relativer Charakter von

¹⁴⁰ PORTMANN/RUDOLPH in BSK, Art. 328b OR N 3; vgl. E. 26 DSGVO.

¹⁴¹ WEBER/OERTLY, N 5.

¹⁴² FLUECKIGER, *Principes généraux*, 7; WEBER/OERTLY, N 9.

¹⁴³ BISSELS/MEYER-MICHAELIS/SCHILLER, 3043.

¹⁴⁴ WEBER/OERTLY, N 34.

¹⁴⁵ BERANEK ZANON, 113.

¹⁴⁶ BAERISWYL, 52.

¹⁴⁷ Botschaft zum Bundesgesetz über den Datenschutz vom 23.03.1988, BBl 1988 II, 413–534, 444–445.

¹⁴⁸ BAERISWYL, 53; BROWN, 217; BISSELS/MEYER-MICHAELIS/SCHILLER, 3043.

Personendaten.¹⁴⁹ Ob eine Information aufgrund zusätzlicher Angaben mit einer Person in Verbindung gebracht werden kann, beurteilt sich aus Sicht der jeweiligen Inhaberin der Information.¹⁵⁰ Bestimmbar ist eine Person, wenn sich ein Personenbezug ohne unverhältnismässigen Aufwand erstellen lässt und auch damit gerechnet werden muss, dass dieser potentiell erfolgt.¹⁵¹ Das Ergebnis hängt vom konkreten Fall ab.¹⁵² Einerseits erleichtern die Möglichkeiten der Technik (z.B. im Internet verfügbare Suchwerkzeuge) die Re-Identifizierung.¹⁵³ Andererseits ist zu berücksichtigen, dass eine algorithmische Rechenoperation, die Milliarden von Daten auf bestimmte Werte hin filtert, Zeit und Energie kostet; ein Unternehmen wird den Algorithmus nur dort einsetzen, wo es erforderlich ist.¹⁵⁴ Dabei wirkt erschwerend, dass die Arbeitgeberin derzeit oft nicht weiss, was für Daten einen guten Arbeitnehmer auszeichnen.¹⁵⁵ Zudem verfügen alle Personendaten über eine Halbwertszeit: Die Identifizierbarkeit nimmt mit der Zeit ab, weil das Interesse an einer personenbezogenen Nutzung und damit der Identifikation sinkt.¹⁵⁶ Es wird in der Lehre teilweise vertreten, dass das Interesse bei reiner Gruppierung bzw. Typologisierung von Arbeitnehmern (auch Singularisierung¹⁵⁷, in Anlehnung an den englischen Wortlaut «singling out» von E. 26 DSGVO, oder Aussondern, entsprechend dem deutschen Wortlaut derselben Bestimmung) fehle: Hier wolle die Arbeitgeberin gar nicht wissen, wer die realen Personen sind, nur z.B., was die Führungsstärke eines bestimmten Typs von Arbeitnehmern auszeichnet. Eine Typologisierung stelle ein Indiz für eine

¹⁴⁹ BGE 136 II 508 = BGer 1C_285/2009 E. 3.2; vgl. Bundesverwaltungsgericht A-3144/2008, E. 2.2.1; ROSENTHAL, Identifizierbarkeit, 202; ders., Entwurf, N 14; PORTMANN/RUDOLPH in BSK, Art. 328b OR N 3; MORSCHER, 175–177.

¹⁵⁰ BGE 136 II 508 = BGer 1C_285/2009 E. 3.4.

¹⁵¹ WEBER/OERTLY, N 6.

¹⁵² BGE 136 II 508 = BGer 1C_285/2009 E. 3.2.

¹⁵³ Ebd.

¹⁵⁴ Vgl. KENYON: How Wechat filters images for one billion users, 14.08.2018, <<https://citizenlab.ca/2018/08/how-wechat-filters-images-for-one-billion-users/>> (besucht am 17.08.2018).

¹⁵⁵ F.A.Z.: Lieber Roboter als Personaler, Frankfurter Allgemeine Zeitung vom 01.03.2018, <<http://www.faz.net/aktuell/beruf-chance/beruf/bewerbersauswahl-durch-den-roboter-gar-nicht-so-abwegig-15473478.html>> (besucht am 05.07.2018).

¹⁵⁶ ROSENTHAL, Identifizierbarkeit, 201.

¹⁵⁷ Ders., Identifizierbarkeit, 198.

Identifizierbarkeit dar, genüge aber alleine nicht zur Berufung des DSG.¹⁵⁸ Wir würden diese Ansicht kritisch hinterfragen, was wir gleich noch erläutern werden.

Entsprechend der beschriebenen Rechtsprechung und Lehre müssten nun beispielsweise bei Fehlen des erforderlichen subjektiven Interesses genetische Daten und IP-Adressen **nicht als Personendaten unter das DSG fallen**, wenn der Arbeitgeberin aggregierte Daten genügen,¹⁵⁹ ebenso wenig das Scanning zum Viren- oder Betrugsschutz oder eine nicht personalisierte Protokollierung des Internet- und E-Mail-Verkehrs.¹⁶⁰ Auch sind produktbezogene von vorgangs- und damit personenbezogenen Überwachungen zu trennen.¹⁶¹ Grundsätzlich kein Interesse der Arbeitgeberin an einer Re-Identifizierung kann nach der beschriebenen Rechtsprechung erkennbar sein, wenn sie aus aggregierten Datenbeständen der Belegschaft generische Muster und Prinzipien für künftige Personalentscheidungen (z.B. Best Practices zu Führungsstilen¹⁶² oder Anforderungsprofile für Führungskräfte¹⁶³) ablesen will. Die beschriebene Rechtsprechung würde voraussichtlich das Vorliegen von Personendaten im Sinne des DSG verneinen, wenn die Arbeitgeberin die Auslastung der Infrastruktur misst, ohne die persönliche Anwesenheit einzelner Arbeitnehmer zu kontrollieren (z.B. Sensor zur Lüftungsregulierung, der den CO₂-Gehalt im Sitzungszimmer misst). Grenzwertig erscheinen jedoch schwarze, an der Unterkante jedes Arbeitstischs angebrachte Kästchen zur Analyse der Arbeitsplatzbenutzung, welche die Bewegungen, Temperatur und Anwesenheitszeiten jedes Arbeitnehmers aufzeichnen. Hier sind eine sorgfältige Prüfung der rechtlichen Zulässigkeit, eine Vorankündigung und Miteinbeziehung der Arbeitnehmer (Art. 6 i.V.m. Art. 48 Abs. 1 lit. a ArG, Art. 10 lit. a MitwG) erforderlich. Ansonsten werden solche Kästchen auf heftige Kritik stossen.¹⁶⁴

¹⁵⁸ Ders., Identifizierbarkeit, 198.

¹⁵⁹ Vgl. ders., Identifizierbarkeit, 198.

¹⁶⁰ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 18.

¹⁶¹ GEISER, 233–234.

¹⁶² So z.B. bei McDonald's: CLASSEN/GÄRTNER, 39.

¹⁶³ Dies z.B. das Ergebnis der Oxygen-Studie von Google: NIKLAS/THURN, 1589.

¹⁶⁴ Z.B. die Kritik gegen das OccupEye beim Daily Telegraph: AJUNWA/CRAWFORD/SCHULTZ, 737.

Selbst wenn obige Beispiele ausserhalb des DSG liegen mögen, ist klarzustellen, dass für den **Prozess der Erhebung und Anonymisierung** auf jeden Fall eine Datenbearbeitung stattfindet, auf die die Grundsätze des DSG anzuwenden sind. Nur der Umgang mit dem Ergebnis der Anonymisierung – den anonymisierten Daten – ist nicht mehr datenschutzrelevant.¹⁶⁵

Einschränkend gilt auch, dass die datenschutzrechtlichen Grundsätze zur Anwendung gelangen, sobald die Analyse mit an sich nicht personenbezogener Zwecksetzung zu personenbezogenen Ergebnissen in Form von **Zufallsfunden** führt.¹⁶⁶

Die Rechtsprechung zum notwendigen subjektiven Interesse an der Re-Individualisierung und die Lehrmeinung, Typologisierungen lägen ausserhalb des DSG, verdienen unserer Meinung nach eine **kritische Hinterfragung**. Zunächst ist darauf hinzuweisen, dass das Bundesgericht im besprochenen konkreten Fall BGE 136 II 508 die IP-Adressen doch als Personendaten qualifiziert hat, weil das Geschäftsmodell des betreffenden Datenbearbeiters, eines Internet-Dienstleisters, ganz eigentlich darauf beruhte, aus den IP-Adressen die Identität von bestimmten Personen abzuleiten.¹⁶⁷ Es war ausreichend, dass die Bestimmbarkeit nur in Bezug auf einen Teil der von der Datenbearbeiterin gespeicherten Informationen gegeben war, um die Daten als Personendaten zu qualifizieren und das DSG zur Anwendung zu berufen.¹⁶⁸ Diese Auslegung stand für das Bundesgericht in Einklang mit der Rechtslage in der Europäischen Union.¹⁶⁹ Sodann ist zu erwähnen, dass von aggregierten Daten für die betroffene Person eine Gefahr ausgehen kann, da die Arbeitgeberin einen informationellen Vorsprung über den Arbeitnehmer erhält, wenn sie weiss, welcher aggregierten Gruppe ein Arbeitnehmer angehört.¹⁷⁰ Sie kann Dienste für ihn personalisieren.¹⁷¹ Der Arbeitnehmer wird messbar

¹⁶⁵ WEBER/OERTLY, N 10.

¹⁶⁶ BAERISWYL, 53.

¹⁶⁷ BGE 136 II 508 = BGer 1C_285/2009 E. 3.5; IP-Adresse ebenfalls als Personendaten qualifiziert von: FLUECKIGER, *Principes généraux*, 6.

¹⁶⁸ BGE 136 II 508 = BGer 1C_285/2009 E. 3.5.

¹⁶⁹ Ebd. E. 3.6 mit Verweis auf Art.-29-Datenschutzgruppe, Personenbezogene Daten, 19.

¹⁷⁰ BODIE *et al.*, 998–999.

¹⁷¹ CROLL: Big data is our generation's civil rights issue, and we don't know it, 31.07.2012, <<http://solveforinteresting.com/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it/>> (besucht am 14.08.2018).

und manipulierbar.¹⁷² Obwohl die betroffenen Arbeitnehmer nach traditionellem Verständnis anonym bleiben, wirkt die Datenbearbeitung direkt auf sie und kann sie in ihrer Persönlichkeit verletzen.¹⁷³ Dies läuft dem Zweck des DSG, dem Schutz der Persönlichkeit (Art. 1 DSG), zuwider. Wir finden es fraglich, ob es im Angesicht von Big Data noch zeitgemäss ist, den Geltungsbereich des DSG auf Fälle zu beschränken, in denen Einzelpersonen individualisierbar sind. Auch individualisierbare Gruppen von Arbeitnehmern können ein Interesse am rechtmässigen Umgang mit Daten haben. Angezeigt wäre, dass der Datenschutz auch hier seine Wirkung entfalten kann. Wenn dem DSG in diesen Fällen trotz der geäusserten Bedenken die Anwendbarkeit versagt bleiben sollte, müssten sich die betroffenen Arbeitnehmer eventualiter auf anderem Weg wehren können. Zu denken ist an die Fürsorgepflicht (Art. 328, Art. 328b OR), den Gesundheitsschutz (Art. 26 ArGV 3) oder den Persönlichkeitsschutz (Art. 28 ZGB). Droht eine Manipulation einer Vielzahl von Personen, ist ein öffentliches Interesse an einer Regulierung, etwa am Schutz der Meinungsfreiheit und Demokratie,¹⁷⁴ denkbar. Das DSG erklärt hier den eidgenössischen Datenschutzbeauftragten für zuständig: Er klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 lit. a DSG). Wenn überwiegende öffentliche Interessen eine widerrechtliche Datenbearbeitung rechtfertigen können (Art. 13 Abs. 1 DSG), müssen sie umgekehrt auch eine an sich rechtmässige Datenbearbeitung verhindern können.

Zwischenfazit: Das DSG ist gemäss bundesgerichtlicher Rechtsprechung auf Bearbeitungen anonymisierter Daten nicht anwendbar, solange die Datenbearbeiterin kein subjektives Interesse an einer Re-Individualisierung hat. Sollte dies gelten, selbst wenn eine Re-Individualisierung technisch ohne unverhältnismässigen Aufwand möglich wäre, so würde ein Grossteil der Bearbeitungen anonymisierter Daten ausserhalb des sachlichen Anwendungsbereichs des DSG erfolgen. Dieses Ergebnis ist unseres Erachtens anzuzweifeln, weil

¹⁷² Vgl. PRIEUR, 1645; vgl. LEWIS PAUL: Senator warns YouTube algorithm may be open to manipulation by «bad actors», The Guardian vom 05.02.2018, <<https://www.theguardian.com/technology/2018/feb/05/senator-warns-youtube-algorithm-may-be-open-to-manipulation-by-bad-actors>> (besucht am 26.11.2018).

¹⁷³ A.M. ROSENTHAL, Identifizierbarkeit, 200.

¹⁷⁴ BOEHME-NESSLER, 111–138.

selbst Bearbeitungen anonymisierter Daten für den einzelnen Arbeitnehmer oder für eine Vielzahl von Arbeitnehmern spürbar nachteilig wirken können.

3. Abgrenzung allgemein zugänglicher und privater Personendaten

In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person ihre **Personendaten allgemein zugänglich** gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 12 Abs. 3 DSGVO).¹⁷⁵ Es handelt sich um eine widerlegbare gesetzliche Vermutung, nicht um eine unumstössliche Fiktion.¹⁷⁶

Die Abstufung zwischen allgemein zugänglichen Daten und solchen, die der Privatsphäre angehören, sei am **Beispiel von individuellen Personalfluktuations-Prognosen** illustriert: Die vorstehend (A.3.b) beschriebenen Anwendungen des Active Sourcings können genauso gut dazu verwendet werden, das Verhalten der eigenen Mitarbeiter im Internet daraufhin zu überprüfen, ob sie abwanderungswillig sind. Die Arbeitgeberin kann für Arbeitnehmer, die sie behalten will, individuell zugeschnittene Mitarbeiter-Bindungsprogramme entwickeln, um der Fluktuation zuvorzukommen.¹⁷⁷

Auszugehen ist von einer Fluktuationsprognose anhand einer Internetrecherche, die ein Mensch mit einer gewöhnlichen Suchmaschine durchführt (sog. **Googlen**). Es ist umstritten, ob die Arbeitgeberin Arbeitnehmer googlen darf, weil sie dabei in der Regel auf Daten stossen wird, die keinen Bezug zum Arbeitsplatz haben.¹⁷⁸ Sie muss ihm gegenüber klar verständigen, dass sie eine solche Nachforschung durchführt.¹⁷⁹ Die Arbeitgeberin darf nicht gezielt

¹⁷⁵ Im weitesten Sinne geht es bei der Qualifikation als allgemein zugängliche Daten um den Rechtfertigungsgrund der konkludenten Einwilligung.

¹⁷⁶ Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017, 6941–7192, 7072.

¹⁷⁷ BISSELS/MEYER-MICHAELIS/SCHILLER, 3043; So z.B. bei SAS (WILSON/BELLIVEAU/GRAY, 31), Microsoft und Xerox (NIKLAS/THURN, 1589).

¹⁷⁸ PIETRUSZAK in KUKO, Art. 328b OR N 9; Das sog. Screening von Stellensuchenden im Internet sei unzulässig, da die Arbeitgeberin dadurch auf Personendaten, die nicht der Eignungsabklärung dienen, stösst und die Datenrichtigkeit nicht gewährleistet ist, PÄRLI in SHK, Art. 328b OR N 28.

¹⁷⁹ FLUECKIGER, Googlelisierung, 82.

nach privaten Daten suchen.¹⁸⁰ Auszuscheiden sind Informationen, die erkennbar gegen den Willen des Arbeitnehmers ins Internet gestellt worden sind.¹⁸¹ Nach einer restriktiven Meinung sollen nur Suchresultate, deren Veröffentlichung der Betroffene explizit wollte, als allgemein zugänglich gemachte Daten gelten.¹⁸² Diese Ansicht erscheint uns realitätsfremd. Andererseits wird argumentiert, mit der Nutzung des Internets korrespondiere eine gewisse Verantwortung und wachsende Netzkompetenz des Betroffenen. Es sei ihm zumutbar, die Verfügbarkeit seiner Daten im Internet zu beobachten und zu steuern.¹⁸³ So oder so müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 Abs. 1 DSG). Wichtig erscheint eine organisatorische Trennung zwischen der Person, welche die Fluktuationsprognose durchführt und dem Personal-Entscheidungssträger, sodass Erstere Letzterem bloss die gefilterten Daten mit Arbeitsplatzbezug zur Kenntnis bringt.¹⁸⁴ Die Arbeitgeberin sollte beim Googlen von Arbeitnehmern immer auf objektive Kriterien abstellen.¹⁸⁵ Alle objektiven Gründe, die für Personalentscheidungen relevant sind, sollten dokumentiert werden.¹⁸⁶

Quasi ein Unterfall des Googlens ist die Suche nach Informationen in den immer beliebteren **sozialen Netzwerken**. Mehr als ein Drittel (36 %) der Unternehmen weltweit überwachte 2012 die Benutzung von sozialen Netzwerken durch die Arbeitnehmer.¹⁸⁷

Die Analyse **berufsbezogener sozialer Netzwerke**¹⁸⁸ erscheint generell zulässig, da die Mitglieder ihr Profil bewusst zu beruflichen Zwecken allgemein zugänglich machen und mit der Einsichtnahme durch einen Personal-

¹⁸⁰ PIETRUSZAK in KUKO, Art. 328b OR N 9.

¹⁸¹ DZIDA, 545.

¹⁸² Vgl. PIETRUSZAK in KUKO, Art. 328b OR N 8, nach welchem in der Regel nicht davon ausgegangen werden könne, dass der Arbeitnehmer Daten, die mit Googlen gefunden werden, allgemein zugänglich gemacht habe; siehe auch, aber **a.M.**: THÜSING/TRAUT, N 7.

¹⁸³ THÜSING/TRAUT, N 16; DZIDA, 545.

¹⁸⁴ PIETRUSZAK in KUKO, Art. 328b OR N 9.

¹⁸⁵ WILDHABER/HÄNSENBERGER, Internet, 328.

¹⁸⁶ Dies., Internet, 328.

¹⁸⁷ AUBERT/DELLEY, 142.

¹⁸⁸ Z.B. LinkedIn oder Xing.

verantwortlichen rechnen.¹⁸⁹ Gleiches muss in Bezug auf Daten von Arbeitnehmern in unternehmensinternen Foren¹⁹⁰ gelten.

Die Zulässigkeit der Analyse **freizeitorientierter sozialer Netzwerke**¹⁹¹ ist umstritten. Restriktiv ist die Haltung, die solche Datenerhebungen wegen des privaten Zwecks des Netzwerks ganz generell verbieten will.¹⁹² Dies gelte unabhängig von den konkreten Datenschutzeinstellungen, da diese oft schwierig zu handhaben seien, und von den Anbietern laufend geändert würden. Selbst bei jüngeren Arbeitnehmern, die mit Social Media aufgewachsen und technisch versiert sind, könne die Arbeitgeberin nicht von einer Zustimmung zur Analyse ausgehen.¹⁹³ Ausser Acht bleibt dabei, dass es jedem frei steht, ein soziales Netzwerk zu verlassen. Mit der Nutzung geht die Selbstverantwortung zur Kontrolle der Einstellungen einher.¹⁹⁴ Nach hier vertretener Meinung kann es nicht allein auf den Zweck des sozialen Netzwerks ankommen, weil gewisse soziale Netzwerke genauso gut zu privaten wie beruflichen Zwecken genutzt werden können.¹⁹⁵ Entscheidend für die Klassifizierung als allgemein zugänglich muss der öffentliche (oder eben private) Charakter der einzelnen Inhalte sein.¹⁹⁶ Orientierungspunkt sind die Umstände des Einzelfalls,¹⁹⁷ insbesondere die Kontoeinstellungen.¹⁹⁸ Zulässig erscheint daher selbst bei freizeitorientierten sozialen Netzwerken die Analyse von Daten, auf die ein praktisch unbegrenzter Kreis von Personen zugrei-

¹⁸⁹ PIETRUSZAK in KUKO, Art. 328b OR N 8; AUBERT/DELLEY, 147; DZIDA, 544.

¹⁹⁰ Z.B. Yammer von Microsoft, SuccessFactors von SAP, Chatter von Salesforce und Workplace von Facebook.

¹⁹¹ Z.B. Facebook.

¹⁹² STUTZ/VALLONI, 5.10; vgl. AUBERT/DELLEY, 158; vgl. STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 10.

¹⁹³ STUTZ/VALLONI, 5.11.

¹⁹⁴ Vgl. EDÖB: Erläuterungen zu sozialen Netzwerken, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html> (besucht am 24.08.2018).

¹⁹⁵ Z.B. Instagram oder Twitter.

¹⁹⁶ Vgl. AUBERT/DELLEY, 157: Facebook stelle sowohl einen öffentlichen als auch einen privaten Raum dar; Der Begriff der Öffentlichkeit wird im Schweizer Recht nicht einheitlich verwendet (vgl. Art. 259 ff. StGB, Art. 652a OR, Art. 54 ZPO, Art. 19 Abs. 1 lit. a URG), WILDHABER/HÄNSENBERGER, Social Media, 408.

¹⁹⁷ Ebd. 407.

¹⁹⁸ AUBERT/DELLEY, 158; PIETRUSZAK in KUKO, Art. 328b OR N 8.

fen kann.¹⁹⁹ Letzteres ist der Fall, wenn die Mitglieder bewusst die Öffentlichkeit suchen und auf die Weiterverbreitung ihrer Mitteilungen keinen Einfluss nehmen.²⁰⁰ Unklar ist, ob die Arbeitgeberin, die nicht direkt mit dem Arbeitnehmer über das soziale Netzwerk befreundet ist, Beiträge einsehen darf, die dieser für «Freunde von Freunden» geöffnet hat.²⁰¹

Im Gegensatz zu einem Menschen, der beim Googlen oder in sozialen Netzwerken nach Informationen sucht, kann ein **Algorithmus zur Internetrecherche** einerseits im Internet Daten aufspüren, die nicht im Sinne von Art. 12 Abs. 3 DSGVO allgemein zugänglich gemacht sind.²⁰² Andererseits kann er allgemein zugängliche Daten zusammenführen, Folgerungen ableiten und Informationen zu Tage fördern, die der Arbeitnehmer so nie offenlegen wollte. Der Arbeitnehmer kann seine Daten gegenüber einer derart ungleich mächtigeren Arbeitgeberin nicht kontrollieren. Entsprechende kommerzielle Dienste zur Kontrolle stehen in der Regel nicht zur Verfügung.²⁰³ Es wird daher vertreten, dass Big-Data-Internetrecherchen, im Gegensatz zum Googlen,²⁰⁴ höchstens im Einzelfall zulässig sein sollten.²⁰⁵ Solch ein Einzelfall wäre z.B. ein Algorithmus, der der Arbeitgeberin zwar Sucharbeit abnimmt, ihr aber im Endeffekt nicht mehr vermittelt, als ein Mensch mit Googlen und genügend Zeit hätte herausfinden können und dürfen.

Zwischenfazit: Ob ein Datum allgemein zugänglich gemacht ist, bestimmt sich nach den konkreten Umständen des Einzelfalls. Grundsätzlich ist an die Selbstverantwortung zu appellieren, die jeder wahrnehmen muss, bevor er persönliche Informationen über sich, welche mit einer gewöhnlichen Suchmaschine auffindbar sind, online schaltet. Die Öffentlichkeit von Informationen ist dort eigenverantwortlich zu steuern, wo die Möglichkeit besteht, entsprechende Einstellungen vorzunehmen. Dies ist bei den meisten sozialen Netzwerken der Fall. Jedoch fehlt die Möglichkeit zu solchen Einstellungen gegenüber einer Arbeitgeberin, die People Analytics einsetzt. People-Ana-

¹⁹⁹ DZIDA, 545.

²⁰⁰ Vgl. BGer 5A_195/2016 E. 5.3 mit Bezug auf Twitter.

²⁰¹ Verneinend: DZIDA, 545.

²⁰² Siehe zum Deep Web Crawler vorstehend, II.A.3.b.

²⁰³ THÜSING/TRAUT, N 29.

²⁰⁴ PIETRUSZAK in KUKO, Art. 328b OR N 9.

²⁰⁵ THÜSING/TRAUT, N 29.

lytics-Anwendungen können Daten aufspüren, die nicht allgemein zugänglich gemacht sind und können allgemein zugängliche Daten zusammenführen und aus der Zusammenführung unerwartete Folgerungen ableiten. Dadurch wird die gesetzliche Vermutung, dass die Bearbeitung allgemein zugänglich gemachter Daten keine Persönlichkeitsverletzung darstelle (Art. 12 Abs. 3 DSG), in manchen Fällen widerlegbar.

4. Verhaltensüberwachung am Arbeitsplatz

Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden (Art. 26 Abs. 1 ArGV 3). **Unzulässig** sind sie, wenn sie ausschliesslich oder vorwiegend die Kontrolle des Verhaltens der Arbeitnehmer bezwecken.²⁰⁶ Ausnahmsweise sind sie zulässig, wenn sie aus andern Gründen erforderlich sind; dann sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3). Der andere Grund muss klar überwiegen.²⁰⁷ Die zweite öffentlich-rechtliche Abteilung des Bundesgerichts hat diese Verordnungsbestimmung des Bundesrats 2004 bestätigt: Entscheidend für die Bestimmung, ob ein Überwachungssystem zulässig ist oder nicht, seien die Beweggründe («motifs»), die für ihre Einführung massgebend waren, und die Zwecke («butts»), welche ihr Einsatz verfolgt, aber weniger die Art («type») der Überwachung und deren Auswirkungen («effets»).²⁰⁸ Das Bundesgericht bestätigte ausdrücklich die Gesetzmässigkeit von Art. 26 ArGV 3.²⁰⁹

In der beschriebenen Rechtsprechung in BGE 130 II 425 erachtete das Bundesgericht ein **GPS-System von damals** als verhältnismässiges Mittel zur Überwachung einer Fahrzeugflotte. Die Arbeitgeberin hatte es zum Zweck des Diebstahlschutzes (E. 5.3), der Arbeitsorganisation (E. 5.4) und der Über-

²⁰⁶ BGE 130 II 425 = BGer 2A.118/2003 = JAR 2005 215 = Pra 2005 Nr. 71 E. 4.4; EMMEL in CHK, Art. 328 OR N 4; PORTMANN/RUDOLPH in BSK, Art. 328b OR N 49; REHBINDER/Stöckli in BK, Art. 328b OR N 29.

²⁰⁷ SECO, 326-2; PIETRUSZAK in KUKO, Art. 328 OR 19a; sogar noch restriktiver: Eine Überwachung ist bereits dann unzulässig, wenn sie *auch* auf das Verhalten der Arbeitnehmer zielt, PORTMANN/RUDOLPH in BSK, Art. 328b OR N 49.

²⁰⁸ BGE 130 II 425 = BGer 2A.118/2003 = JAR 2005 215 = Pra 2005 Nr. 71 E. 4.1.

²⁰⁹ Ebd. E. 3.3.

prüfung der Arbeitsverrichtung (E. 5.5) in ihren Fahrzeugen installiert. Das System zeichnete die geografische Position des Fahrzeugs auf und wie lange es bei einem Kunden parkiert war. Es liess jedoch keine Schlüsse zu, wie oder ob ein Arbeitnehmer seine Arbeit verrichtete, weshalb die Gefahr einer Verhaltensüberwachung limitiert war (E. 5.5.1–5.5.2).

Heutige GPS-Systeme zeichnen das Verhalten wesentlich detaillierter auf: Die Sensoren eines internationalen Postzulieferers lokalisieren die Fahrzeuge, verwerten geografische Daten (z.B. Adressen, Landkarten) und erheben Daten über die Pakete (z.B. Absende- und Zustellungszeitpunkt). Gestützt darauf errechnet ein Algorithmus die kürzeste Fahrstrecke für die zu verteilenden Pakete. Dadurch sinken Treibstoffverbrauch und Fahrerbedarf und steigt die Anzahl zugestellter Pakete.²¹⁰ Die Sensoren melden im Voraus, wann Fahrzeugteile ersetzt werden müssen (sog. Preventative Maintenance).²¹¹ Sie zeichnen auch auf, wann der Fahrer die Tür öffnet, das Fahrzeug sichert, wann sein Fuss das Bremspedal berührt, wann der Motor leer läuft und wann der Fahrer die Sicherheitsgurte anschnallt.²¹²

Dient das beschriebene heutige GPS-System zu einem wesentlichen Teil der Verhaltensüberwachung und ist es somit nach Art. 26 ArGV 3 verboten? Für die Beantwortung dieser Frage ist ein **jüngeres Urteil** aus dem Jahr 2009 massgeblich. Die strafrechtliche Abteilung des Bundesgerichts hat entschieden, dass es an einer genügenden Delegationsnorm in einem Gesetz im formellen Sinn, die den Bundesrat zum Erlass einer Verordnungsnorm zur Überwachung der Arbeitnehmer am Arbeitsplatz ermächtigen würde, fehlt (vgl. Art. 182 Abs. 1 BV).²¹³ Daher ist Art. 26 Abs. 1 ArGV 3 einschränkend

²¹⁰ KONRAD ALEX: Meet Orion, software that will save UPS millions by improving drivers' routes, Forbes vom 01.11.2013, <<https://www.forbes.com/sites/alexkonrad/2013/11/01/meet-orion-software-that-will-save-ups-millions-by-improving-drivers-routes/>> (besucht am 03.04.2018); AJUNWA/CRAWFORD/SCHULTZ, 743–744.

²¹¹ ZAX: Brown down: UPS drivers vs. the UPS algorithm, 01.03.2013, <<https://www.fast-company.com/3004319/brown-down-ups-drivers-vs-ups-algorithm>> (besucht am 12.04.2018).

²¹² Z.B. das Telematik-System On-Road Integrated Optimization and Navigation (ORION) des Postzulieferers United Parcel Service (UPS): BRUDER: These workers have a new demand: Stop watching us, 27.05.2015, <<https://www.thenation.com/article/these-workers-have-new-demand-stop-watching-us/>> (besucht am 12.04.2018).

²¹³ BGer 6B_536/2009 E. 3.3.2; STREIFF/VON KAENEL/RUDOLPH, 335 m.w.H.

auszulegen: Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden, wenn sie geeignet sind, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen.²¹⁴ Entscheidend ist das Kriterium der Gesundheitsbeeinträchtigung (BGer 6B_536/2009 E. 3.6.2). Diese ist nicht eo ipso gegeben, wenn ein Überwachungssystem (hauptsächlich) der Überwachung dient (E. 3.6.2). Neben dem Zweck sind insbesondere die Häufigkeit und die Dauer der Überwachung massgebend und bei welchen Tätigkeiten der Arbeitnehmer vom System erfasst wird (E. 3.4.1). Weitere Kriterien sind die eingesetzte Technik, verwendete Datenmenge, Zugänglichkeit der Informationen und welche Relevanz die Daten hinsichtlich des Persönlichkeitsrechts des Betroffenen aufweisen (Sensibilität der Informationen, Anzahl betroffener Persönlichkeitsaspekte).²¹⁵ Daher kann ein Überwachungssystem, das den Arbeitnehmer nur sporadisch und kurzzeitig bei bestimmten Gelegenheiten erfasst, erlaubt sein, obwohl es (hauptsächlich) der gezielten Überwachung des Verhaltens der Arbeitnehmer am Arbeitsplatz dient.²¹⁶ Die Überwachung muss im Vergleich zum beabsichtigten Zweck ein verhältnismässiges Mittel (Art. 4 Abs. 2 DSGVO) darstellen.²¹⁷ Verboten wird die generelle Verhaltensüberwachung sein.²¹⁸

Bei heutigen GPS-Ausrüstungen von Flotten ist somit zu prüfen, ob aus ihnen eine **überwachende Wirkung** und damit eine Gesundheitsbeeinträchtigung für die Arbeitnehmer resultiert. Ob eine überwachende Wirkung in der Absicht der Arbeitgeberin liegt und dem Sinn der technischen Einrichtung entspricht, ist unerheblich.²¹⁹ Bei einem System wie dem oben beschriebenen, das den Fahrer anweist, die Sicherheitsgurte anzuschallen, *bevor* er den Motor anlässt, um Benzin zu sparen, und welches für eine geringe Abwei-

²¹⁴ BGer 6B_536/2009 E. 3.6.1; MORSCHER, 189–190; PORTMANN/RUDOLPH in BSK, Art. 328b OR 50a.

²¹⁵ WILDHABER, 219.; vgl. WOLFER, N 182–197

²¹⁶ BGer 6B_536/2009 E. 3.6.2; PORTMANN/RUDOLPH in BSK, Art. 328b OR 50a; PIETRUSZAK in KUKO, Art. 328 OR 19a.

²¹⁷ PORTMANN/RUDOLPH in BSK, Art. 328b OR N 49; Es geht beim Verbot der Verhaltensüberwachung letztendlich um die Verhältnismässigkeit im engeren Sinn, d.h. eine Abwägung zwischen Zweck und Wirkung, so auch DONAUER/MÖRI, 1057.

²¹⁸ STUTZ/VALLONI, 5.45.

²¹⁹ WILDHABER, 219.

chung von der algorithmisch optimalen Route eine Rechtfertigung verlangt, ist unseres Erachtens eine überwachende Wirkung gegeben. Problematisch sind Geolokalisierungs-Sensoren, die der Arbeitnehmer direkt auf sich trägt. So binden sich Lagerhallenarbeiter Paketscanner (sog. Picker) an den Unterarm, die ihnen helfend den Weg zum Lagergang und Regal für das nächste Paket weisen, aber zugleich die Arbeitsgeschwindigkeit vorschreiben²²⁰ und bei Pausen ausserhalb der regulären Zeiten Alarm schlagen.²²¹ Ein Kriterium für die Einstufung der überwachenden Wirkung muss auch der Datenzugriff sein: Kann sich der Arbeitnehmer selbst mit seiner Leistung in der Vergangenheit vergleichen, ist People Analytics eine Hilfe zum Selbstmanagement. Können dagegen auch Vorgesetzte und Arbeitskollegen die Resultate einsehen, entsteht Stress. Auch der gut gemeinte Ansatz, Arbeit zu einem Wettbewerb gleich einem Spiel auszugestalten, bei dem alle im Unternehmen permanent gegenseitig ihren Punkte- bzw. Spielstand sehen (sog. Gamification²²²), entfaltet eine überwachende Wirkung.

Zwischenfazit: Die Verhaltensüberwachung mit People Analytics ist nicht a priori unzulässig. Entscheidend ist, sie verhältnismässig einzusetzen, z.B. mit Stichproben anstelle von permanenter Überwachung.

C. People Analytics nach Beendigung des Arbeitsverhältnisses

Der Schutz der Personendaten des Arbeitnehmers (Art. 328b OR) gilt nicht nur während des Arbeitsverhältnisses, sondern genauso und ohne zeitliche Befristung danach.²²³ Somit sind die **Grundsätze des DSG** anwendbar (Art. 328b Satz 2 OR). Die Daten sind unaufgefordert²²⁴ zu vernichten, sobald sie für den Zweck, der zu ihrer Erhebung geführt hat, nicht mehr benötigt werden (vgl. Art. 4 Abs. 3 DSGVO).

²²⁰ Z.B. bei Federal Express (FedEx): BRUDER, FN 211.

²²¹ WILDHABER, 219; z.B. bei Amazon: AJUNWA/CRAWFORD/SCHULTZ, 744; HOLTHAUS/PARK/STOCKHOMBURG, 676.

²²² AJUNWA/CRAWFORD/SCHULTZ, 770; BODIE *et al.*, 974–975.

²²³ BGE 131 V 298 E. 6.1.

²²⁴ Zur DSGVO: FRANZEN, 327.

Zu prüfen ist, ob es einen Rechtfertigungsgrund für eine Bearbeitung von Personendaten über die Beendigung des Arbeitsverhältnisses hinaus gibt. In Frage kommen eine Einwilligung, ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Bestimmung (Art. 13 Abs. 1 DSGVO). Für eine gültige rechtfertigende **Einwilligung** (1. Variante von Art. 13 Abs. 1 DSGVO) in eine Datenbearbeitung gelten nach Vertragsbeendigung die gleichen Voraussetzungen wie vor Stellenantritt. Art. 328b OR ist analog anwendbar, wenn die Arbeitgeberin Dossiers abgewiesener Bewerber aufbewahren will.²²⁵ Nur mit der Zustimmung der Bewerber dürfen ihre Unterlagen für eine bestimmte, im Voraus festgelegte Dauer aufbewahrt werden, wenn anzunehmen ist, dass die Daten demnächst wieder gebraucht werden.²²⁶ Die Einwilligung ist erst gültig, wenn sie nach angemessener Information freiwillig und, bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, zudem ausdrücklich erfolgt (Art. 4 Abs. 5 DSGVO). Bei Bewerbern mag die Freiwilligkeit fehlen, weil sie zustimmen müssen, um sich die Chancen auf den Job aufrechtzuerhalten. Hingegen ist eine freiwillige Zustimmung bei beendigem Arbeitsverhältnis rechtlich gesehen vorstellbar, da die für laufende Arbeitsverträge und Bewerbungsverfahren typische Machtasymmetrie entfällt. Die Einwilligung muss sich auf eine bestimmte Dauer und einen bestimmten Bearbeitungszweck beziehen.

Eine befristete Aufbewahrung kommt aus **überwiegenden Interessen** (2. Variante von Art. 13 Abs. 1 DSGVO) in Frage, etwa in Anbetracht offener Rechtsstreitigkeiten²²⁷ oder zur Durchsetzung eines Konkurrenzverbotes.²²⁸ Nur diejenigen Daten dürfen aufbewahrt werden, die dazu weiterhin erforderlich (Art. 328b Satz 1 OR) sind. Die Aufbewahrungsdauer ist je nach Datenkategorie einzeln festzulegen und beträgt ohne gesetzlich bestimmte Frist zwei²²⁹ bis fünf Jahre.²³⁰

In Betracht fallen schliesslich **gesetzliche Pflichten** (3. Variante von Art. 13 Abs. 1 DSGVO), die eine Aufbewahrung von Personendaten rechtfertigen. Zu

²²⁵ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 13.

²²⁶ EDÖB, Personendaten, 11.

²²⁷ EMMEL in CHK, Art. 328b OR N 6.

²²⁸ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 13.

²²⁹ MATHYS, 100.

²³⁰ EDÖB, Personendaten, 14.

denken ist an die Ausstellung oder spätere Berichtigung eines Zeugnisses und die Erteilung von Referenzen (Art. 330a OR). Die Pflicht zur zehnjährigen Aufbewahrung der Geschäftsbücher (Art. 958f OR) kann E-Mails erfassen, wenn diese entsprechende Daten enthalten.²³¹ Sie kann aber nicht als Rechtfertigungsgrund für eine allgemeine E-Mail-Aufbewahrung greifen, wenn bloss ein kleiner Teil der E-Mails Informationen zu den Geschäftsbüchern enthält.²³² Art. 328b OR ist in diesem Fall *lex specialis*.²³³ Gleiches muss in Bezug auf andere gesetzliche, etwa sozialversicherungs-, steuer- oder aufsichtsrechtliche Aufbewahrungspflichten gelten. Z.B. müssen Banken zwar aufsichtsrechtliche Pflichten wie die Sicherstellung der Gewähr (Art. 3 Abs. 2 lit. c BankG) erfüllen. Der EDÖB schritt jedoch gegen eine schweizerische Grossbank ein, die eine Datensammlung mit sicherheitsrelevanten Daten²³⁴ über Mitarbeiter, Kunden und Dritte, zum Teil ohne deren Kenntnis führte.²³⁵ Der EDÖB empfahl, die Personendaten frühestmöglich zu löschen oder zu anonymisieren.²³⁶ Unzulässig wäre es unseres Erachtens, People Analytics dazu einzusetzen, aus den (nicht anonymisierten) Daten eines erfolglosen Ex-Arbeitnehmers ein Profil unerwünschter Bewerber zu erstellen, oder ihn auf eine Sperrliste zu setzen, um seinen Wiedereintritt in einer anderen Unternehmensabteilung oder Konzerngesellschaft zu verhindern.

Zwischenfazit: Die Datenbearbeitung ist nach Beendigung des Arbeitsverhältnisses grundsätzlich unzulässig und kann nur in Ausnahmefällen gerechtfertigt werden. Anwendungen von People Analytics müssen dieses «Ablaufdatum» berücksichtigen und Mitarbeiterdaten rechtzeitig löschen oder anonymisieren.

²³¹ DUNAND, 58.

²³² Vgl. MATHYS, 100.

²³³ STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 13.

²³⁴ EDÖB, Schlussbericht, 3.

²³⁵ EDÖB, Schlussbericht, 1.

²³⁶ EDÖB, Schlussbericht, 12.

III. Schlusswort

Big Data und People Analytics bringen riesige Herausforderungen für das Recht der Privatsphäre am Arbeitsplatz. Es besteht die Gefahr, dass die Arbeitgeberin den Arbeitnehmer unverhältnismässig überwachen kann – Big Brother is watching you. Das heutige Rechtssystem kommt bei People Analytics aber an seine Grenzen. Es besteht rechtlicher Klärungsbedarf in einer Vielzahl von Einzelfragen, das hat sich klar gezeigt.

Trotz der offenen Rechtsfragen und grossen Herausforderungen geht die laufende DSGVO-Revision die Big-Data-Problematik nicht an. Der Bundesrat hat 2015 die Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» beauftragt, Klarheit über die Auswirkungen von Big Data zu schaffen.²³⁷ Er hat den Schlussbericht dieser Expertengruppe am 5. September 2018 zur Kenntnis genommen und das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) beauftragt, bis Mitte 2019 die insgesamt 51 Empfehlungen der Expertengruppe zu analysieren und dem Bundesrat entsprechende Folgearbeiten zum Entscheid zu unterbreiten.²³⁸ Im Schlussbericht finden sich leider keine Empfehlungen bezüglich People Analytics.²³⁹ Umso gespannter blicken wir künftig auf die Tätigkeit eines anderen Eidgenössischen Departements: dasjenige für Wirtschaft, Bildung und Forschung (WBF). Das dem WBF angegliederte Staatssekretariat für Wirtschaft SECO ist für die Arbeitsmarktpolitik zuständig und könnte sich der Thematik People Analytics annehmen.

Die Zulässigkeit von People Analytics hängt von zahlreichen Variablen im Einzelfall ab (z.B. geschäftliche oder private Aktivitäten als Kontrollobjekt, verdeckte oder angekündigte Kontrollen, permanente Überwachung oder Stichproben, Zweck(e) der Kontrolle).²⁴⁰ Somit können in vielen Fällen nur die Gerichte angemessene Entscheidungen für den konkreten Fall treffen. Aber

²³⁷ PRIEUR, 1643.

²³⁸ Schweizerischer Bundesrat: Bundesrat nimmt Schlussbericht der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» zur Kenntnis, 10.09.2018, <<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-72083.html>> (besucht am 22.11.2018).

²³⁹ Vgl. Schweizerischer Bundesrat, 7–13.

²⁴⁰ Vgl. PORTMANN/RUDOLPH in BSK, Art. 328b OR N 41.

People Analytics verbreitet sich derart rasant und betrifft so viele Personen in ihren Rechten, dass es unseres Erachtens nicht nur den Gerichten überlassen werden sollte. Es braucht eine öffentliche politische Diskussion der offenen Fragen. Auch wenn sich die Beteiligten bisweilen bereits an die «Verdatung» des Arbeitslebens gewöhnt haben mögen, sind für diese Diskussion auch die Gefahren von People Analytics für die Gesundheit und Privatsphäre der Einzelnen sowie für das Vertrauensklima im Betrieb zu traktandieren.

Literatur

- AJUNWA IFEOMA/CRAWFORD KATE/SCHULTZ JASON: Limitless worker surveillance, *California Law Review* 2017, 735–776.
- Art.-29-Datenschutzgruppe: Opinion 2/2017 on data processing at work, Brüssel 08.06.2017 (zit. Data processing).
- Art.-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», Brüssel 20.06.2007 (zit. Personenbezogene Daten).
- ARYANI HEDYA: The legal implications of biodata use as an employment selection practice, *University of Pennsylvania Journal of Business Law* 2009, 1051–1073.
- AUBERT CAROLE/DELLEY RÉGINE: Utilisations des réseaux sociaux par les travailleurs et les employeurs, in: Dunand Jean-Philippe/Mahon Pascal (Hg.): *Internet au travail*, Genf 2014, 131–163.
- BAERISWYL BRUNO: Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf H./Thouvenin Florent (Hg.): *Big Data und Datenschutz – gegenseitige Herausforderungen*, Zürich/Basel/Genf 2014, 45–59.
- BAUMANN ROBERT: Die Übertragung von Arbeitnehmerdaten bei Betriebsübergängen, *Aktuelle Juristische Praxis* 2004, 638–648.
- BERANEK ZANON NICOLE: Big Data und Datensicherheit, in: Weber Rolf H./Thouvenin Florent (Hg.): *Big Data und Datenschutz – gegenseitige Herausforderungen*, Zürich/Basel/Genf 2014, 85–115.
- BISSELS ALEXANDER/MEYER-MICHAELIS ISABEL/SCHILLER JAN: Arbeiten 4.0: Big Data-Analysen im Personalbereich, *Der Betrieb* 2016, 3042–3049.
- BODIE MATTHEW T./CHERRY MIRIAM A./McCORMICK MARCIA L./JINTONG TANG: The law and policy of people analytics, *University of Colorado Law Review* 2017, 961–1042.
- BOEHME-NESSLER VOLKER: Die Macht der Algorithmen – Anmerkungen zum Einfluss von Big Data auf die Demokratie, in: Boehme-Nessler Volker/Rehbinder Manfred (Hg.): *Big Data: Ende des Datenschutzes?*, Bern 2017, 111–138.
- BROWN ELIZABETH A.: Workplace wellness: Social injustice, *New York University Journal of Legislation and Public Policy* 2017, 191–246.
- BSK. Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (Hg.): *Obligationenrecht I*, Art. 1–529 OR, 6. A., Basel 2015 (zit. Bearbeiter in BSK).

- BSK. Maurer-Lambrou Urs/Blechta Gabor P. (Hg.): Datenschutzgesetz, Öffentlichkeitsgesetz, 3. A., Basel 2014 (zit. Bearbeiter in BSK).
- BSK. Maurer-Lambrou Urs/Vogt Nedim Peter (Hg.): Datenschutzgesetz, 2. A., Basel 2006 (zit. Bearbeiter in BSK).
- CHK. Huguenin Claire/Müller-Chen Markus (Hg.): Handkommentar zum Schweizer Privatrecht, Vertragsverhältnisse Teil 2: Arbeitsvertrag, Werkvertrag, Auftrag, GoA, Bürgschaft, 3. A., Zürich/Basel/Genf 2016 (zit. Bearbeiter in CHK).
- CLASSEN MARTIN/GÄRTNER CHRISTIAN: Im Kampf um Big Data, personalmagazin 2016, 38–39.
- COSTA GIORDANO: Internet- und E-Mail-Überwachung am Arbeitsplatz, Jusletter 09.01.2012.
- CUSTERS/CALDER/SCHERMER/ZARSKY: Discrimination and privacy in the information society, Berlin/Heidelberg 2013.
- DAEDELLOW ROMY: Beschäftigtendatenschutz und DSGVO, digma – Zeitschrift für Datenrecht und Informationssicherheit 2017, 34–37.
- DONAUER DANIEL/MÖRI BARBARA A.: Die privatrechtliche Fürsorgepflicht des Arbeitgebers und rechtliche Konsequenzen, Aktuelle Juristische Praxis 2015, 1049–1061.
- DUNAND JEAN-PHILIPPE: Internet au travail: droits et obligations de l'employeur et du travailleur, in: Dunand Jean-Philippe/Mahon Pascal (Hg.): Internet au travail, Genf 2014, 33–72.
- DZIDA BORIS/GRAU TIMON: Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG – Zehn Fragen aus der Praxis, Der Betrieb 2018, 189–194.
- DZIDA BORIS: Big Data und Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht 2017, 541–546.
- EDÖB: Leitfaden über die Bearbeitung von Personendaten im Arbeitsbereich, Bern 10.2014 (zit. Personendaten).
- EDÖB: Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz, Bern 09.2013 (zit. Internet und E-Mailüberwachung).
- EDÖB: Schlussbericht betreffend die Datenbearbeitung im Zusammenhang mit der Datensammlung [...] von [...] AG, Bern 03.06.2014 (zit. Schlussbericht).
- FLUECKIGER CHRISTIAN: La googlelisation des employés respecte-t-elle les principes de la protection des données?, in: Dunand Jean-Philippe/Mahon Pascal (Hg.): Internet au travail, Genf 2014, 73–97 (zit. Googlelisation).
- FLUECKIGER CHRISTIAN: Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail, in: Dunand Jean-Philippe/Mahon Pascal (Hg.): La protection des données dans les relations de travail, Genf 2017, 1–23 (zit. Principes généraux).
- FRANZEN MARTIN: Datenschutz-Grundverordnung und Arbeitsrecht, Europäische Zeitschrift für Arbeitsrecht 2017, 311–351.

- GEISER THOMAS: Rechte und Pflichten von Banken und Bankmitgliedern in Verfahren vor Behörden und Gerichten (Datenherausgabe, Unterstützungspflichten, Schadenersatz), Zeitschrift des bernischen Juristenvereins 2016, 231–260.
- GUENOLE NIGEL/FERRAR JONATHAN/FEINZIG SHERI: The power of people, Glenview, Illinois 2017.
- HKDSG. Rosenthal David/Jöhri Yvonne (Hg.): Handkommentar zum Datenschutzgesetz, sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit. Bearbeiter in HKDSG).
- HOFMANN KAI: Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, Zeitschrift für Datenschutz 2016, 12–17.
- HOLTHAUS CHRISTIAN/PARK YOUNG-KUL/STOCK-HOMBURG RUTH: People Analytics und Datenschutz – Ein Widerspruch?, Datenschutz und Datensicherheit 2015, 676–681.
- HUGENTOBLE MARKUS: Datenschutzfalle Assessment Center, Aktuelle Juristische Praxis 2009, 153–156.
- KAINER FRIEDEMANN/WEBER CHRISTIAN: Datenschutzrechtliche Aspekte des «Talentmanagements», Betriebs-Berater 2017, 2740–2747.
- KAISER STEPHAN: Roboter statt Recruiter?, personalmagazin 2014, 12–15.
- KIM PAULINE T./HANSON ERIKA: The law and business of people analytics: People analytics and the regulation of information under the fair credit reporting act, Saint Louis University Law Journal 2016, 17–33.
- KIM PAULINE T.: Data-driven discrimination at work, William & Mary Law Review 2017, 587–936.
- KUKO. Honsell Heinrich (Hg.): Kurzkomentar Obligationenrecht, Art. 1–1186, Basel 2014 (zit. Bearbeiter in KUKO).
- MATHYS ROLAND: Big Data in der Rechtspraxis, in: Epiney Astrid/Nüesch Daniela (Hg.): Big Data und Datenschutzrecht / Big data et le droit de la protection des données, Zürich 2016, 95–102.
- MEIER PHILIPPE: Protection des données, Bern 2011.
- MÉTILLE SYLVAIN: La surveillance électronique des employés, in: Dunand Jean-Philippe/Mahon Pascal (Hg.): Internet au travail, Genf 2014, 99–129.
- MORSCHER LUKAS: Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, Zeitschrift des bernischen Juristenvereins 2011, 177–221.
- NIKLAS THOMAS/THURN LUKAS: Arbeitswelt 4.0 – Big Data im Betrieb, Betriebs-Berater 2017, 1589–1596.
- OFK. Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc/Fankhauser Roland (Hg.): OR Kommentar, Schweizerisches Obligationenrecht, 3. A., Zürich 2016 (zit. Bearbeiter in OFK).
- PAPA ROBERTA/PIETRUSZAK THOMAS: Datenschutz im Personalwesen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hg.): Datenschutzrecht, Basel 2015, 577–611.
- PÄRLI KURT: Datenaustausch zwischen Arbeitgeber und Versicherung: Probleme der Bearbeitung von Gesundheitsdaten der Arbeitnehmer bei der Begründung des privatrechtlichen Arbeitsverhältnisses, Bern 2003 (zit. Datenaustausch).

- PRIEUR YVONNE: Datenschutz durch «Big-Data-Geschäfte» auf dem Prüfstand, Aktuelle Juristische Praxis 2015, 1643–1653.
- REHBINDER MANFRED/STÖCKLI JEAN-FRITZ: Berner Kommentar zu den Art. 319–330b OR, Bern 2010.
- REINSCH ROGER W./GOLTZ SONIA: The law and business of people analytics: Big data: Can the attempt to be more discriminating be more discriminatory instead?, Saint Louis University Law Journal 2016, 35–63.
- RIEMER-KAFKA GABRIELA: Datenschutz zwischen Arbeitgeber und Versicherungsträgern, Schweizerische Juristen-Zeitung 2000, 285–293.
- RIESELMAHN-SAXER REBEKKA: Datenschutz im privatrechtlichen Arbeitsverhältnis, Bern 2002.
- ROSENTHAL DAVID: Der Entwurf für ein neues Datenschutzgesetz, Jusletter 27.11.2017 (zit. Entwurf).
- ROSENTHAL DAVID: Personendaten ohne Identifizierbarkeit?, digma – Zeitschrift für Datenrecht und Informationssicherheit 2017, 198–203 (zit. Identifizierbarkeit).
- SCHWEIZERISCHER BUNDESRAT: Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Bern 17.08.2018.
- SECO: Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Bern 05.2018.
- SHK. Baeriswyl Bruno/Pärlä Kurt (Hg.): Datenschutzgesetz (DSG), Bern 2015 (zit. Bearbeiter in SHK).
- SNYDER TIMOTHY M.: You're fired! A case for agency moderation of machine data in the employment context, George Mason Law Review 2016, 243–283.
- STRAHILEVITZ LIOR JACOB: Toward a positive theory of privacy law, Harvard Law Review 2013, 2010–2042.
- STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER: Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. A., Zürich 2012.
- STUTZ MICHÈLE/VALLONI NOEMI: Social Media im Arbeitsrecht, in: Staffelbach Oliver/Keller Claudia (Hg.): Social Media und Recht für Unternehmen, Zürich 2015, 159–187.
- SUBILIA OLIVIER/DUC JEAN-LOUIS (Hg.): Droit du travail, 2. A., Lausanne 2010.
- THÜSING GREGOR/TRAUT JOHANNES: Social Media in Betrieb und Unternehmen, in: Thüsing Gregor (Hg.): Beschäftigtendatenschutz und Compliance, München 2014, 1–69.
- WEBER ROLF H./OERTLY DOMINIC: Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?, in: Weber Rolf H. (Hg.): Datenschutz – zum Aufstieg einer neuen Rechtsdisziplin, Bern 2015.
- WESPI ANDREAS: Big Data: Technische Perspektive, in: Weber Rolf H./Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 3–16.
- WILDHABER ISABELLE/HÄNSENBERGER SILVIO: Internet am Arbeitsplatz, Zeitschrift des bernischen Juristenvereins 2016, 307–341 (zit. Internet).
- WILDHABER ISABELLE/HÄNSENBERGER SILVIO: Kündigung wegen Nutzung von Social Media, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hg.): Recht im digitalen Zeitalter, Zürich 2015, 399–430 (zit. Social Media).

WILDHABER ISABELLE: Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, Aktuelle Juristische Praxis 2017, 213–224.

WILDHABER ISABELLE: Die Roboter kommen – Konsequenzen für Arbeit und Arbeitsrecht, Zeitschrift für Schweizerisches Recht 2016, I, 315–351 (zit. Roboter).

WILSON REBECCA J./BELLIVEAU KILEY M./GRAY LEIGH ELLEN: Busting the black box: Big data, employment and privacy, Defense Counsel Journal 2017, 2–34.

WOLFER: Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich 2008.

ZÜST MARTIN: Big brother's watching you at work, Aktuelle Juristische Praxis 1996, 1475–1487.