Internet- und E-Mail-Überwachung am Arbeitsplatz

Entwicklungen in der Lehre, Rechtsprechung und Gesetzgebung

- Autor: Giordano Costa
- Rechtsgebiete: Datenschutz

Zitiervorschlag: Giordano Costa, Internet- und E-Mail-Überwachung am Arbeitsplatz, in: Jusletter 9. Januar 2012

Die Lehre hat den Leitfaden des EDöB über die Internet- und E-Mail-Überwachung am Arbeitsplatz weitgehend bestätigt. Die personenbezogene Auswertung der Logfiles dient nicht der Feststellung eines Missbrauchs oder der Begründung eines konkreten Missbrauchsverdachts, sondern lediglich der darauffolgenden, punktuellen Identifikation des verantwortlichen Arbeitnehmers. Dabei darf das Verhalten eines Arbeitnehmers retrospektiv über eine längere Zeitspanne offengelegt werden. Spionprogramme oder die ständige namentliche Auswertung der Logfiles sind hingegen nicht zulässig. Der Bund hat die Grundsätze des Leitfadens in der Revision des RVOG berücksichtigt.

Inhaltsverzeichnis

1.

Einführung ^

[Rz 1]
Die Einführung des Internets und der elektronischen Post am Arbeitsplatz hat sich zweifellos positiv auf die Produktivität von Unternehmen und öffentlichen Verwaltungen ausgewirkt. Dennoch versuchen Arbeitgeber aus einer instinktiven Abwehrhaltung heraus und im Bestreben, ihre durch die elektronischen Medien potentiell tangierten Interessen[1] zu schützen, deren Nutzung unter Kontrolle zu halten. Man spricht diesbezüglich allgemein von Internet- und E-Mail-Überwachung am Arbeitsplatz.
[Rz 2]
Die Überwachung als Grundhaltung gegenüber Gefahren ist im Arbeitskontext nicht unproblematisch. Tatsächlich kann die Überwachung einen unzulässigen Eingriff in die Persönlichkeit des Arbeitnehmers darstellen. Die Schwere der Persönlichkeitsverletzung ist bedeutender, wenn besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile betroffen sind, wie dies bei der Benutzung von Internet und E-Mail häufig der Fall ist. Stuft der Arbeitgeber seine Eigentumsrechte an der elektronischen Infrastruktur und deren Schutz grundsätzlich höher ein als die Persönlichkeitsrechte der betroffenen Personen, kann hieraus oft eine Persönlichkeitsverletzung resultieren.[2] Bei einer solchen Gewichtung der Rechtsgüter geht der Arbeitgeber normalerweise davon aus, dass er den Arbeitnehmer mehr oder weniger vorbehaltlos überwachen darf. In einem solchen Fall spielt der Persönlichkeitsschutz des Arbeitnehmers in den Augen des Arbeitgebers sowohl bei der Normierung als auch bei der Durchführung der Internet- und E-Mail-Überwachung am Arbeitsplatz eine untergeordnete Rolle.
[Rz 3]
Die nationale und internationale Datenschutzgemeinschaft hat bereits vor gut zwölf Jahren angefangen, die datenschutzrechtliche Problematik der Internet- und E-Mail-Überwachung am Arbeitsplatz genauer zu untersuchen. In der Schweiz wurde diesbezüglich vor etwa zehn Jahren der Leitfaden des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) betreffend Internet- und E-Mail-Überwachung am Arbeitsplatz (nachfolgend Leitfaden) erstmals publiziert[3].

[Rz 4]
Ein wichtiger Teil des Leitfadens, welcher weiterhin als einer der Hauptbeiträge der Schweizer Praxis in dieser Materie gilt, befasst sich damit, dass die personenbezogene Auswertung der Logfiles nicht zur Feststellung eines Internet- oder E-Mail-Missbrauchs am Arbeitsplatz (bzw. zur Gründung eines entsprechenden konkreten Verdachts) herangezogen, sondern nach festgestelltem Sachverhalt zur Identifikation des fehlbaren Arbeitnehmers vorgenommen werden darf.
[Rz 5]
Ob sich dieser Grundsatz bis heute halten und durchsetzen konnte, versucht folgende Analyse über die entsprechenden bisherigen Entwicklungen in der Lehre, Rechtsprechung und Gesetzgebung zu beantworten.

2.

Der Leitfaden in Kürze ^

2.1

Der Leitfaden als Minimalstandard ^

[Rz 6]
Im Leitfaden wird das herrschende Bundesrecht betreffend den Persönlichkeitsschutz des Arbeitnehmers erklärt und konkretisiert. Er setzt sich insbesondere mit Art. 26 der Verordnung vom 18. August 1993 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3, SR 822.113) betreffend das Verbot der Verhaltensüberwachung der Angestellten am Arbeitsplatz, auseinander. Diese Bestimmung gilt sowohl für öffentliche Verwaltungen von Bund, Kantonen und Gemeinden als auch für die Privatwirtschaft (Art. 3a und 6 Abs. 4 Bundesgesetz vom 13. März 1964 über die Arbeit in Industrie, Gewerbe und Handel, Arbeitsgesetz, ArG, SR 822.11). Sofern in den folgenden Ausführungen ausdrücklich nichts anderes vorbehalten wird, betrifft der Begriff des Arbeitgebers somit sowohl den Bund als auch die Kantone, die Gemeinden und die privaten Unternehmen.
[Rz 7]
Der Leitfaden stellt nicht nur ein Dokument zur Sensibilisierung dar, sondern ist eine Auslegungshilfe, insbesondere für Art. 26 ArGV 3 und generell für die rechtlichen Bestimmungen zum Persönlichkeitsschutz, wobei die Ausführungen zu Art. 328 ff. OR lediglich für die Anstellungsverhältnisse in der Privatwirtschaft gelten. Obwohl der Leitfaden keine Rechte und Pflichten wie eine Rechtsnorm begründet[4], dürfen ihn weder die öffentlichen Verwaltungen, noch die Privatwirtschaft ignorieren, wenn sie kein Einschreiten der Datenschutzbehörden des Bundes oder der Kantone riskieren wollen. Mit anderen Worten gibt der Leitfaden den Willen des Gesetzgebers wieder und gibt damit einen Minimalstandard für die Internet- und E-Mailüberwachung vor.

2.2

Überwachungsverfahren ^

[Rz 8]
Gemäss Leitfaden soll der Arbeitgeber den verantwortlichen Arbeitnehmer identifizieren und zur Verantwortung ziehen können, falls dieser die Regeln der Internet- und E-Mail-Nutzung am Arbeitsplatz verletzt hat oder entsprechende konkrete Anzeichen hierfür bestehen. Der Rechtfertigungsgrund der personenbezogenen Auswertung liegt im überwiegenden Interesse des Arbeitgebers an der Klärung des Sachverhalts und der Verantwortlichkeiten im Falle der Verletzung seiner Interessen. Der Leitfaden sieht zwei Überwachungsverfahren vor: Die präventive Überwachung (Kapitel 8 des Leitfadens) und die punktuelle namentliche Analyse der *Logfiles* aufgrund von Hinweisen, die nicht im Rahmen einer präventiven Überwachung aufgekommen sind (ansatzweise in den Kapiteln 7.2 und 8.2 des Leitfadens beschrieben). Die Lehre benutzt zum Teil andere Begriffe für diese Unterscheidung und spricht etwa von globaler Kontrolle einerseits und gezielter bzw. personenbezogener Überwachung andererseits[5].
[Rz 9]
Die präventive Überwachung ist fix vorgegeben. Deren einzelne Etappen verlaufen in eine bestimmte Richtung und dürfen nicht durcheinander gebracht werden[6]. Danach dürfen Missbräuche (bzw. entsprechende konkrete Verdachtsmomente) in einer ersten Phase ausschliesslich durch eine nicht personenbezogene Auswertung der *Logfiles* festgestellt werden. Die Lehre folgt diesen Ansatz[7]. Diese Phase spielt sich in ständiger bzw. in zeitlich beschränkter (oder periodischer) Art und Weise ab, je nach dem, ob sie anonymisiert oder pseudonymisiert vorgenommen wird[8].
[Rz 10]
Erst beim Aufdecken eines Missbrauchs oder beim Entstehen eines konkreten Missbrauchsverdachts in dieser Phase kann der Arbeitgeber in der nächsten Phase die *Logfiles* personenbezogen auswerten. Anders als die nicht personenbezogene Auswertung, darf die personenbezogene Auswertung der *Logfiles* lediglich punktuell durchgeführt werden. Die personenbezogene Auswertung, d.h. im Endeffekt die rechtlich relevante Verhaltensüberwachung, weist mit anderen Worten keinen Dauerhaftigkeitscharakter auf, obwohl sie bei entsprechender Vornahme das Verhalten eines Arbeitnehmers über eine längere Zeitspanne offenlegen kann. Die retrospektive personenbezogene Auswertung der

Logfiles nach Feststellung eines Missbrauchs oder nach Entstehen eines konkreten Missbrauchsverdachts in der nichtpersonenbezogenen Phase ist somit zulässig[9].
[Rz 11]
Die Verhinderung des Dauerhaftigkeitscharakters einer personenbezogenen Überwachung wird auch bei anderen Überwachungsmethoden, wie bspw. bei der Video-[10], Kassen-[11] oder Mitarbeiterkontenüberwachung, angestrebt. Auch das Bundesgericht erachtet die zeitliche Komponente einer Überwachungsmassnahme als massgebend für deren Rechtmässigkeit im Lichte von Art. 26 ArGV 3[12].
[Rz 12]
Sie stellt ein Mittel zur Reduzierung der Persönlichkeitsverletzung auf ein vertretbares Minimum dar. Die personenbezogene Auswertung der *Logfiles* darf daher nicht für die Feststellung eines Missbrauchs oder für die Begründung eines konkreten Missbrauchsverdachts herangezogen werden, sondern lediglich in der Folge verwendet werden. Sie ist mit anderen Worten ausschliesslich zur Identifikation des fehlbaren Arbeitnehmers gedacht, wenn ein Verstoss bereits festgestellt wurde. Daraus lässt sich bspw. ableiten, dass das personenbezogene Ausspionieren der Arbeitnehmer (egal, ob mit oder ohne vorherige Missbrauchsfeststellung oder konkreten Missbrauchsverdacht), bspw. durch Spionprogramme oder ständige namentliche Auswertung der *Logfiles*, verboten ist[13].
[Rz 13]
Neben der präventiven Überwachung sieht der Leitfaden die punktuelle personenbezogene Analyse der *Logfiles* als weiteres Überwachungsverfahren vor. Letzteres wird durch Missbrauchshinweise ausgelöst, die nicht im Rahmen einer präventiven Überwachung entdeckt worden sind und in der Regel keiner bestimmten oder bestimmbaren Person zugewiesen werden können[14].

2.3

Analogie der Internet- und E-Mail-Überwachung zum Auswertungsverfahren einer Black Box? ^

[Rz 14]
Bei den gerade beschriebenen Überwachungsverfahren wird manchmal die Analogie zur Auswertung der Black Box eines Flugzeuges[15] herangezogen und entsprechend von einem Black Box-Prinzip (oder Ursache-Folge-Prinzip) bei der Internet- und E-Mail-Überwachung am Arbeitsplatz gesprochen. Danach dürfen die *Logfiles* nur dann ausgewertet werden, wenn ein Auslöser (d.h. ein Vorfall wie eine technische Störung oder ein Missbrauch) bereits besteht.
[Rz 15]
Es ist diesbezüglich allerdings zu präzisieren, dass vom Black Box Prinzip ausschliesslich in Zusammenhang mit der personenbezogenen Auswertung der *Logfiles* gesprochen werden kann, da die nicht personenbezogene Auswertung der Internet- und E-Mail-*Logfiles* – anders als die Black Box-Daten – auch ohne Auslöser (d.h. ohne Missbrauch oder konkreten Missbrauchsverdacht) möglich ist.

3.

Die bundesrechtlichen Grundlagen der Internet- und E-Mail-Überwachung am Arbeitsplatz ^

3.1

De lege data ^

[Rz 16]
Jede Überwachung von Personen, mit welcher Technik auch immer, geht mit einer Persönlichkeitsverletzung einher, weshalb eine gesetzliche Grundlage als Rechtfertigungsgrund erforderlich ist, wie dies das Bundesgericht in seinem 2009 gefällten Urteil[16] betreffend Videoüberwachung im öffentlichen Raum (Kanton Bern) festgehalten hat. Speziell zur Videoüberwachung hat es ausgeführt, dass der Grad der Persönlichkeitsverletzung je nach angewandter Methode (z.B. mit oder ohne Echtzeitüberwachung und/oder Bildaufnahmen) variieren kann, dass aber in jedem Fall eine Persönlichkeitsverletzung entsteht, da dadurch die Sammlung von Informationen (z.B. über die Anwesenheit einer Person an einem bestimmten Ort, ihr Verhalten, ihre Gewohnheiten und soziale Beziehungen) im weiten Sinne des Wortes ermöglicht wird.
[Rz 17]
Da die Persönlichkeitsverletzung einen gemeinsamen Nenner sämtlicher Überwachungsarten darstellt, können diese Schlussfolgerungen des Bundesgerichtes ebenfalls auf die Internet- und E-Mail-Überwachung am Arbeitsplatz angewendet werden. Diese setzt so, zumindest im öffentlichen Bereich, gesetzliche Grundlagen voraus[17].

3.2

Art. 328 ff. OR ^

[Rz 18]
Die nachfolgenden Ausführungen zu den Art. 328 ff. des Schweizerischen Obligationenrechts (OR, SR 220) betreffen ausschliesslich privatrechtliche Arbeitsverhältnisse. Auf die Arbeitsverhältnisse bei Bund, Kantonen und Gemeinden gelten die Persönlichkeitsschutzbestimmungen der entsprechenden Personal- und/oder Datenschutzgesetzgebung (für das Arbeitsverhältnis beim Bund siehe insb. Art. 4 Abs. 2 lit. g Bundespersonalgesetz, BPG, SR 172.220.1).
[Rz 19]
Im Schweizerischen Privatrecht wird der Persönlichkeitsschutz des Arbeitnehmers in erster Linie in den Art. 328 und 328b OR geregelt. Diese Bestimmungen, welche als *lex specialis* gegenüber den generell-abstrakten Bestimmungen des Bundesgesetzes über den Datenschutz (DSG, RS 235.1) gelten, sehen in allgemeiner, jedoch klarer Form, einerseits die Pflicht des Arbeitgebers vor, die Persönlichkeit des Arbeitnehmers zu schützen und zu achten (Art. 328 OR). Andererseits wird diese Pflicht durch das Recht des Arbeitgebers dahingehend vervollständigt und präzisiert, dass er jene Daten, die zur Abklärung der Eignung für das Arbeitsverhältnis oder zur Durchführung des Arbeitsvertrages nötig sind, bearbeitet werden dürfen (Art. 328b OR).
[Rz 20]
Das Bundesgericht hat in einem Urteil zur GPS-Ortung[18] durch ein privates Unternehmen diesbezüglich präzisiert, dass nicht jede Methode oder jedes Instrument zur Erhebung dieser an sich zulässigen Daten erlaubt ist. Die Datenerhebungsmethode muss ebenfalls – so das Bundesgericht – die Persönlichkeit des Arbeitnehmers gemäss Art. 328 OR respektieren und die generellen Rechtsgrundsätze, insbesondere das Transparenz- und Verhältnismässigkeitsprinzip, beachten. Unter mehreren möglichen Methoden muss der Arbeitgeber also diejenige wählen, welche am wenigsten in die Persönlichkeit des Arbeitnehmers eingreift. Damit hat das Bundesgericht den Leitfaden des EDÖB insofern generell bestätigt, dass die Internet- und E-Mailüberwachung am Arbeitsplatz in einer für die Persönlichkeit schonenden Art und Weise zu erfolgen hat. Im gleichen Sinne äussert sich auch die Lehre[19].
[Rz 21]
Die Schlussfolgerungen des Bundesgerichtes gelten analog selbstverständlich auch für die Anstellungsverhältnisse bei Bund, Kantonen und Gemeinden.

3.3

Art. 26 ArGV 3 ^

[Rz 22]
Wie das Bundesgericht in einem 2009 gefällten Urteil[20] festgehalten hat, enthält das Arbeitsgesetz keine Bestimmungen betreffend die Überwachung der Arbeitnehmer am Arbeitsplatz. Es enthält auch keine Bestimmung, die den Bundesrat ausdrücklich zum Erlass von Vorschriften auf dem Gebiet der Überwachung der Arbeitnehmer am Arbeitsplatz ermächtigt. Es erstaunt – so das Bundesgericht –, dass der heikle und schwierige Gegenstand der Überwachung der Arbeitnehmer am Arbeitsplatz lediglich in einer bundesrätlichen Verordnung geregelt wird, und zwar in einer Verordnung, die sich auf das Arbeitsgesetz stützt, welches seinerseits den Begriff der Überwachung überhaupt nicht enthält. Es wäre zu begrüssen, wenn die Überwachung der Arbeitnehmer am Arbeitsplatz zumindest in den Grundzügen in einem Gesetz im formellen Sinne geregelt würde.
[Rz 23]
Die öffentlichrechtliche Gesundheitsvorsorgegesetzgebung (Art. 26 der Verordnung 3 vom 18. August 1993 zum Arbeitsgesetz, Gesundheitsvorsorge, ArGV 3, SR 822.113) – welche, wie bereits festgehalten, sowohl für privatrechtliche als auch für öffentlichrechtliche Arbeitsverhältnisse von Bund, Kantonen und Gemeinden gilt – sieht für die Überwachung am Arbeitsplatz eine Spezifizierung vor[21]. Danach dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden (Abs. 1). Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden (Abs. 2).
[Rz 24]
Inhaltlich legt Art. 26 ArGV 3 im ersten Absatz in allgemeiner Form das Verbot einer Verhaltensüberwachung fest, und behält im zweiten Absatz die Überwachung aus anderen Gründen[22] vor. Es wird also lediglich zwischen unzulässiger Verhaltensüberwachung und zulässiger Überwachung aus anderen Gründen unterschieden. Eine Unterscheidung zwischen den verschiedenen, im Leitfaden beschriebenen Methoden der Verhaltensüberwachung (bspw. zwischen personenbezogener und nicht personenbezogener Verhaltensüberwachung oder zwischen personenbezogener Auswertung mit oder ohne vorherige Missbrauchsfeststellung oder konkreten Missbrauchsverdacht) wird hingegen nicht getroffen, sondern es ist nur vom Verhaltensüberwachungsverbot die Rede.
[Rz 25]
Die grammatikalische Auslegung dieser Norm lässt somit auf ein absolutes Verbot der Verhaltensüberwachung schliessen.
[Rz 26]
Das Bundesgericht hat im GPS-Urteil Art. 26 ArGV 3 untersucht und sich zum Verhältnis zwischen den Art. 328 ff. OR dahingehend geäussert, dass diese Bestimmung nicht nur die physische und psychische Gesundheit des Arbeitnehmers

zum Schutzobjekt hat, sondern ebenfalls seine persönliche Integrität, d.h. seine Persönlichkeit im Sinne von Art. 328 ff. OR. Die Lehre kommt mehrheitlich zum gleichen Schluss[23].
[Rz 27]
Die oberste Gerichtsinstanz hat zudem allgemein festgehalten, dass gemäss Art. 26 ArGV 3 ein Überwachungssystem dann verboten ist, wenn es ausschliesslich oder hauptsächlich das Verhalten der Arbeitnehmer zum Gegenstand hat[24]. Dem Arbeitgeber wird aber weiter das Recht zuerkannt, die Einhaltung seiner internen Richtlinien betreffend Leistung und Verhalten am Arbeitsplatz mit adäquaten Mitteln kontrollieren zu können[25]. Die Lehre bestätigt ebenfalls diese Einschätzung[26].
[Rz 28]
Damit ist die Verhaltensüberwachung nach Auffassung des Bundesgerichts und der Lehre – ganz im Sinne des Leitfadens – rechtlich grundsätzlich möglich. Das Verhaltensüberwachungsverbot ist mit anderen Worten nicht absolut. Dies wird auch in einem anderen Bundesgerichtsentscheid bestätigt, wonach die Massnahme zur Verhaltensüberwachung nur dann gegen das Verhaltensüberwachungsverbot verstösst, sofern sie geeignet ist, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen[27]).
[Rz 29]
Konkrete Anhaltspunkte, wie die Internet- und E-Mailüberwachung am Arbeitsplatz rechtmässig gestaltet werden soll, liefert die Rechtsprechung des Bundesgerichts nicht.
[Rz 30]
Zurzeit ist ein Fall von Internetüberwachung am Arbeitsplatz vor dem Tessiner Obergericht hängig, aus dem weitergehende Präzisierungen betreffend die Internet- und E-Mail-Überwachung am Arbeitsplatz zu erhoffen sind.
[Rz 31]
Der Leitfaden hat seinerseits bezüglich Art. 26 ArGV 3 bereits vor zehn Jahren eine teleologische Interpretation geliefert, welche nicht nur die Rechte des Arbeitnehmers, sondern auch diejenigen des Arbeitgebers in die Überlegungen mit einbezieht[28]. Wie bereits festgehalten, ist es demnach für den Arbeitgeber rechtlich möglich, die Einhaltung des Nutzungsreglements betreffend Internet- und E-Mail zu kontrollieren, sofern dabei die Persönlichkeit des Arbeitnehmers nicht widerrechtlich verletzt wird[29].

3.4

De lege ferenda ^

[Rz 32]
Auch im Rahmen der Gesetzgebung des Bundes hat der Leitfaden Eingang gefunden. Seine Grundsätze finden sich in der Revision des Regierungs- und Verwaltungsorganisationsgesetzes des 21. März 1997 (RVOG, SR 172.010) wieder. Damit wird ein rechtlicher Rahmen für die Überwachung der Angestellten des Bundes angestrebt. Die Revision wurde am 10. Oktober 2010 durch das Parlament genehmigt (BBl 2010 6579) und wird, parallel zum Erlass der materiell-rechtlichen Ausführungsbestimmungen, voraussichtlich anfangs 2012 in Kraft treten[30].
[Rz 33]
Der Gesetzesentwurf übernimmt die Schlüsselelemente des Leitfadens betreffend die Analysemethoden im Hinblick auf die Voraussetzungen für die Internet- und Email-Überwachung am Arbeitsplatz bei der punktuellen Analyse und der präventiven Überwachung. Diese sind für die präventive Überwachung die anonyme Analyse (nArt. 57m) sowie die pseudonyme Analyse (nArt. 57n) und für die punktuelle Analyse die personenbezogene Auswertung (nArt. 57o).
[Rz 34]
Konkret wird künftig der Bund als Arbeitgeber Personendaten aufzeichnen dürfen, die bei der Nutzung seiner oder der in seinem Auftrag betriebenen elektronischen Infrastruktur entstehen. Es wurde also, vor allem aus technischen Gründen, von einem Verbot mit Erlaubnisvorbehalt abgesehen und sich für eine generelle Erlaubnis mit abschliessender Auflistung der Datenbearbeitungszwecke entschieden.
[Rz 35]
Wünschenswert wäre es, dass der Bundesgesetzgeber ebenfalls die Mitarbeiterüberwachung in der Privatwirtschaft gesetzlich (bspw. im ArG) regeln, bzw. konkretisieren würde[31].

4.

Die kantonalrechtlichen Grundlagen der Internet- und E-Mail-Überwachung am Arbeitsplatz ^

[Rz 36]
Da die Mitarbeiterüberwachung nicht eine rein bundespersonalrechtliche Angelegenheit ist, wird der kantonale Gesetzgeber sie ebenfalls regeln müssen.
[Rz 37]
Die Richtlinien des Leitfadens wie auch das revidierte RVOG können dabei als Modell herangezogen werden.
[Rz 38]

Die Mehrheit der Kantone hat die Grundsätze des Leitfadens, und somit das geltende Recht, in eigenen Gesetze oder Richtlinien übernommen[32]. Bei einigen Kantonen ist die Regelung der Internet- und E-Mail-Überwachung allerdings nicht mit dem geltenden öffentlichen Arbeitsrecht konform[33]. Andere Kantone wiederum verfügen noch über keine Regelung[34].

5.

Fazit ^

[Rz 39]
Die Lehre hat den Leitfaden des EDÖB über die Internet- und E-Mail-Überwachung am Arbeitsplatz in seinem Grundsatz weitgehend bestätigt. Die personenbezogene Auswertung der *Logfiles* wird somit als punktuelle (Identifikations-) Massnahme verstanden, welche erst nach Aufdecken eines Missbrauchs oder nach Entstehen eines konkreten Missbrauchsverdachts in der präventiven Überwachungsphase durchgeführt werden darf. Die personenbezogene Auswertung kann das Verhalten eines Arbeitnehmers retrospektiv über eine längere Zeitspanne offenlegen. Das personenbezogene Ausspionieren des Arbeitnehmers (egal, ob mit oder ohne vorherige Missbrauchsfeststellung oder konkreten Missbrauchsverdachts), bspw. durch Spionprogramme oder ständige personenbezogene Auswertung der *Logfiles*, ist hingegen verboten. Die Rechtsprechung in dieser Materie ist jedoch noch nicht gefestigt[35]. Gesetzgeberisch haben sowohl der Bund als auch mehrere Kantone bereits rechtliche Grundlagen für die Internet- und E-Mail-Überwachung am Arbeitsplatz erlassen oder sind dran, dies zu tun. Die anderen Kantone, welche noch keine gesetzlichen Grundlagen erarbeitet haben, bzw. derzeit über eine nicht rechtskonforme Regelung verfügen, müssen dies nachholen bzw. ihre bestehenden Grundlagen anpassen.
[Rz 40]
Ideal wäre es, die Mitarbeiterüberwachung in der Privatwirtschaft und in den öffentlichen Verwaltungen gesamtschweizerisch einheitlich auf formeller Ebene (in der öffentlichen Arbeitsgesetzgebung des Bundes, bspw. im ArG), zu verankern.

Lic. iur. Giordano Costa ist wissenschaftlicher Mitarbeiter des Datenschutzbeauftragten des Kantons Tessin.

1. 1Bspw. die Speicherkapazität, der Netzwerkdurchsatz, die Datensicherheit oder die finanziellen Interessen.
2. 2So bspw. in der Dienstanweisung des Kantons SG vom 25. August 2009 über den Einsatz und die Verwendung von Informatikmitteln.
3. 3http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=de
4. 4Vgl. BELSER/NOUREDDINE, in BELSER/EPINEY/WALDMANN, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 439, N 71.
5. 5Siehe BERTIL COTTIER, in DUNAND, SUBILIA, PASCE, COTTIER, STOLL, Internet au lieu de travail, CEDIDAC, Lausanne 2004, S. 98.
6. 6Vgl. ebenfalls DAVID ROSENTHAL in DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 328b OR, N 103.
7. 7Vgl. bspw. CHRISTOF HOHLENSTEIN, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) am Arbeitsplatz, Bern 2002, § 16.
8. 8Zur anonymen und pseudonymen Überwachung, vgl. Leitfaden, Kapitel 8, sowie MARTIN WINTERBERGER-YANG, Basler Kommentar, Datenschutzgesetz, 2. Auflage, Basel 2006, Art. 328b/362 OR, N23.
9. 9Andere Meinung: Bericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2010, S. 14 ff.
10. 10Vgl. Erläuterungen des EDÖB zur Videoüberwachung am Arbeitsplatz, insb. § 3 (Privacy Filters), http://www.edoeb.admin.ch/themen/00794/00800/00911/index.html?lang=de.
11. 11Zur Auswertung von Protokollierungen der Kassenaktivitäten zur Klärung von Inventurdifferenzen, siehe 12. Tätigkeitsbericht des EDÖB, Kapitel 7.1.
12. 12Urteil des Bundesgerichts 6B_536/2009 vom 12. November 2009, Erw. 3.4.1 und 3.6.2
13. 13Die Verordnung des Kantons ZH vom 17. September 2003 über die Nutzung von Internet- und E-Mail sieht aber eine namentliche, dauerhafte Überwachung in Echtzeit vor.

    Zur Problematik der namentlichen, dauerhaften Überwachung in Echtzeit siehe ebenfalls MEIER, S. 690, N 2145.
14. 14Bspw. das Vorfinden von gedrucktem privatem Material beim Firmendrucker oder eine Zeugenaussage gegen unbekannte Arbeitnehmer.
15. 15Die Black Box hält sämtliche Flugdaten für die allfällige Klärung eines Flugzeugunfalls oder schweren Zwischenfalls fest.
16. 16Urteil des Bundesgerichts 1C_315/2009 vom 13. Oktober 2010. Zur Notwendigkeit von gesetzlichen Grundlagen bei Grundrechtseingriffen siehe ebenfalls sinngemäss BGE 126 I 50 (Eingriffe in das Fernmeldegeheimnis).
17. 17Im privaten Arbeitsbereich gilt hauptsächlich die Einwilligung als Rechtfertigungsgrund.
18. 18BGE 130 II 425.
19. 19Vgl. bspw. PHILIPPE MEIER, Protection des données, Bern 2011, S. 689, N 2144.

20. 20Urteil des Bundesgerichts 6B_536/2009 vom 12. November 2009, Erw. 3.3.2
21. 21Siehe dazu Motion Reimann 84.598 Persönlichkeitsschutz des Arbeitnehmers; Amtliches Bulletin des Nationalrates: http://www.amtsdruckschriften.bar.admin.ch/loadDocQuery.do?context=results&documentIndex=0&dsUID=9cbd4b:1312e130b70:-7194#detailView. Vgl. ebenfalls die Wegleitung des Seco zu den Verordnungen 3 und 4 des Arbeitsgesetzes, http://www.seco.admin.ch/dokumentation/publikation/00009/00027/01625/index.html?lang=de.
22. 22Z.B. zur Sicherheits- oder Leistungskontrolle.
23. 23Vgl. bspw. MEIER S. 663, N 2077 und 2139. Gegenteilige Meinung: REBEKKA RIESSELMANN-SAXER, Datenschutz im privatrechtlichen Arbeitsverhältnis, Bern 2002, § 13, S. 108 ff.
24. 24GPS-Urteil, Erw. 4.4. Vgl. ebenfalls MEIER, S. 687, N 2140 und 2143.
25. 25Vgl. GPS-Urteil, Erw. 4.2.
26. 26Vgl. bspw. DAVID ROSENTHAL, Art. 328b OR, N 96 ff., und HOHLENSTEIN, § 16, S. 117.
27. 27Siehe Urteil des Bundesgerichts 6B_536/2009 vom 12. November 2009, Erw. 3.6.1
28. 28Insbesondere das Weisungsrecht des Arbeitgebers, Art. 321d Obligationenrecht, OR, SR 220.
29. 29Vgl. ebenfalls HOHLENSTEIN, § 16, S. 118.
30. 30Details zur Revision des RVOG sind unter der Webseite des Bundesamtes für Justiz zu finden: http://www.bj.admin.ch/content/bj/de/home/dokumentation/medieninformationen/2008/ref_2008-12-120.html
31. 31Auch im Sinne des BGE 6B_536/2009, Erw. 3.3.2
32. 32So bspw. GE, JU, NE, ZH, TI, VS, SG, BS, ZG, SO, AG, Stadt Zürich.
33. 33Kantone SG und TI.
34. 34So bspw. GR und AR.
35. 35Die bestehende Rechtsprechung hat meistens nur die arbeitsrechtlichen Konsequenzen eines Internetmissbrauchs, nicht jedoch die Überwachungsprozedur zum Gegenstand. Siehe bspw. Urteile des Bundesgerichts 4C.173/2003 vom 21. Oktober 2003, 4C.463/1999 vom 4. Juli 2000, 4C.349/2002 vom 25. Juni 2003, sowie Arrêts du Tribunal administratif de la République et Canton de Genève, ATA/496/2006 (19. September 2006) et ATA/618/2010 (7. September 2010).