Big Data-Überwachung am Arbeitsplatz – Grenzen der Zulässigkeit durch aktuelle Gerichtsentscheidungen

Nicolai Culik und Lukas Forte, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Westfälische Wilhelms-Universität Münster

1 Einführung

Für Big Data, also die schnelle Verarbeitung umfangreicher und unterschiedlicher Datenbestände, gibt es auch im Arbeitsverhältnis Anwendungsbedarf. Der Nutzen liegt nämlich grundsätzlich darin, aus der Vergangenheit Schlüsse zu ziehen, um bestmögliche Entscheidungen für die Zukunft zu treffen. Durch die kombinierte und systematische Analyse allerhand Randparameter werden bestimmte Abhängigkeiten und Muster erkannt, die im jeweiligen Zusammenhang genaue Prognosen zulassen.

a) Big Data im Personalwesen

Auch Personalentscheidungen sind das Ergebnis eines Analyse-Prozesses und stellen eine Prognose dar. In einem Bewerbungsgespräch wird versucht, sich ein Bild davon zu machen, wie erfolgreich der Bewerber später arbeiten wird und welchen Nutzen er dem Unternehmen voraussichtlich einbringt. In diesem Zusammenhang gibt es Ansätze, sich weniger auf das eigene Bauchgefühl, als auf errechnete Korrelationen zu verlassen. Zeigt sich beispielsweise, dass besonders erfolgreiche Mitarbeiter bestimmte Charaktereigenschaften aufweisen oder spezielle Qualifikationen mitbringen, könnte es Sinn ergeben, diese Merkmale bei der Bewerberauswahl stärker zu gewichten. Die Ermittlung der Daten muss dafür nicht länger allein klassisch durch Bewerbungsunterlagen und Gespräch erfolgen. Durchgeführt werden können z.B. auch Online-Background-Checks, etwa durch das automatisierte Abfragen sozialer Netzwerke.

Doch nicht nur zur Bewerberauswahl können Big Data-Anwendungen im Personalwesen eingesetzt werden. Schließlich erfolgt ein Großteil der Auswahlentscheidungen in Unternehmen im Zuge der Beförderung oder Versetzung von Mitarbeitern oder bei der Zusammenstellung von Projektteams. Weitere Zwecke der Analyse können Laufbahnplanung, Teamentwicklung, Trainingsbedarfsanalyse, Standortbestimmung oder Potenzialanalyse sein. Auch dafür ist es von großem Nutzen, Leistungsdaten des betroffenen Arbeitnehmers zu messen und in die Entscheidung einfließen zu lassen. In seinem erst kürzlich ergangenen Urteil zog das Bundesarbeitsgericht Grenzen der rechtlichen Zulässigkeit (BAG 2017). Speziell ging es dabei um den Einsatz von Keyloggern.

Abstract / Key Findings

- Big Data findet im Personalwesen vermehrt Anwendung, etwa zu Zwecken der Bewerberauswahl oder der Optimierung von Arbeitsabläufen.
- Das Datenschutzrecht zieht für die Erhebung und Verarbeitung von Beschäftigtendaten allerdings Grenzen, die kürzlich vom Bundesarbeitsgericht und dem Europäischen Gerichtshof für Menschenrechte gestärkt wurden.
- Keylogger bspw. dürfen zur Überwachung der Arbeitnehmer nicht heimlich eingesetzt werden. Dies gilt auch bei Verdacht der übermäßig privaten Nutzung des Dienst-PCs, sodass Kündigungen, die sich auf derart gewonnene Informationen stützen, unwirksam sind.
- Vielmehr muss für die heimliche Informationsbeschaffung ohne Einwilligung des Betroffenen ein konkreter Verdacht einer schweren Pflichtverletzung oder einer Straftat vorliegen; ansonsten sind Einwilligungen einzuholen oder Betriebsvereinbarungen abzuschließen.
- Diese Anforderungen an die Überwachung von Arbeitnehmern sind höher als bspw. in den USA und haben auch zukünftig trotz europäischer und nationaler Änderungen im Datenschutzrecht Bestand.

b) Was ist Keylogging?

Keylogger (dt. „Tasten-Protokollierer“) erfassen sämtliche Tastenanschläge und Eingaben des PC-Nutzers und senden diese in regelmäßigen Abständen an den eingestellten Empfänger. So ist es möglich, Screenshots von allen auf dem Bildschirm des PC-Nutzers verfolgten Aktivitäten zu übermitteln und sogar die Webcam unerkennbar zu öffnen und Bilder des PC-Nutzers aufzunehmen (Ciampa 2017: 85).

Zwei Arten von Keyloggern können unterschieden werden: Hardwarebasierte Keylogger erfordern eine unmittelbare physische, z.B. drahtgebundene, Verbindung zum Betriebssystem und schalten sich zwischen Tastatur und Rechner. Die erlangten Daten werden dabei in einem integrierten Speicher gesammelt. Bei den softwarebasierten bzw. drahtlosen Keyloggern werden die Tastenanschläge stattdessen regelmäßig unverschlüsselt per Funkübertragung an den PC versandt, sodass ein Angreifer die Daten ohne größeren Aufwand abfangen und die getätigten Eingaben rekonstruieren kann (Vogelsang et al. 2016: 730). Im vor dem Bundesarbeitsgericht verhandelten Fall setzte der Arbeitgeber einen solchen softwarebasierten Keylogger ein. Diese Keylogging-Technik wird meist von Hackern als Virus oder Trojaner installiert, um Unternehmensdaten auszuspähen oder vertrauliche Daten der Nutzer, wie Kennwörter, PINs, Kreditkartennummern und Zugänge zu Benutzeraccounts, abzufangen (Gabler Lexikon 2017).

2 Aktuelles Urteil des Bundesarbeitsgerichts

Im Fokus stand bei dem Gerichtsverfahren die Frage, ob die aus dem heimlichen Einsatz eines Keyloggers zur Aufzeichnung der Aktivitäten des Arbeitnehmers gewonnen Daten für eine Kündigung verwendet werden dürfen.

a) Sachverhalt der Entscheidung

In dem Verfahren vor dem Bundesarbeitsgericht wehrte sich ein Web-Entwickler gegen die Kündigung seiner Agentur. Diese hatte der Belegschaft im Zusammenhang mit der Freigabe eines neuen WLAN-Netzwerks mitgeteilt, dass nunmehr sämtliches Datenaufkommen (sog. „Traffic“) aufgezeichnet und dauerhaft gespeichert werde, um rechtlichem Missbrauch vorzubeugen, bzw. um diesen aufzuklären. Zu diesem Zweck wurde auf dem Dienst-PC des Arbeitnehmers auch heimlich ein Keylogger installiert, der dessen Surf-Verhalten protokollierte und speicherte.

Durch Auswertung der Log-Dateien gelang es der Agentur herauszufinden, dass der Arbeitnehmer das Internet und seine Arbeitszeit in erheblichem Umfang für private Zwecke nutzte, z.B. die Programmierung eines Computerspiels oder die Verwaltung von Aufträgen aus dem Unternehmen seines Vaters. Daraufhin kündigte der Arbeitgeber das Arbeitsverhältnis außerordentlich und fristlos. Dagegen wehrte sich der Arbeitnehmer mit dem Argument, das durch den heimlichen Einsatz der Keylogging-Technik gewonnene Datenmaterial sei rechtswidrig erworben worden und könne daher nicht als Grundlage für seine Kündigung dienen.

b) Hohe Anforderungen an heimliche Datenerhebung am Arbeitsplatz

Das Bundesarbeitsgericht entschied, dass eine derartige Ausspähung einen schweren Eingriff in das Grundrecht des Arbeitnehmers auf informationelle Selbstbestimmung darstelle. Dieses umfasse auch das Recht auf die eigene Bestimmung über Preisgabe und Verwendung seiner persönlichen Daten (Pressemitteilung BAG 2017). Das Bundesdatenschutzgesetz (BDSG) erlaubt in seinem § 32 Abs. 1 S. 2 eine Informationsgewinnung im Hinblick auf personenbezogene Daten ohne Einwilligung des Betroffenen nur unter strengen Voraussetzungen. Eine Datenerhebung und -nutzung darf danach einzig durchgeführt werden, wenn gegen den Arbeitnehmer ein konkreter Verdacht einer Straftat oder einer schweren Pflichtverletzung während der Arbeitszeit besteht und die Verarbeitung erforderlich ist. Dazu ist zu prüfen, ob das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht die Informationsinteressen des Arbeitgebers überwiegen, insbesondere ob Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Richter waren der Auffassung, dass die Maßnahme des Arbeitgebers „ins Blaue hinein“ durchgeführt wurde, ohne dass ein vorher objektiv begründeter Verdacht gegen den Arbeitnehmer bestand. Darüber hinaus

ist die Verhältnismäßigkeit der Maßnahme in Frage zu stellen (so bereits die Vorinstanz LAG Hamm 2016). Vor dem Hintergrund der hohen Intensität des Eingriffs durch die heimliche Aufzeichnung sämtlicher Tastenanschläge und besuchter Webseiten käme als milderes Mittel zunächst eine Kontrolle im Beisein des Arbeitnehmers in Betracht (LAG Hamm 2016: Rn. 40). Da die Aufzeichnung aus den genannten Erwägungen rechtswidrig war, lehnten die Richter die aus dem Keylogging gewonnenen Log-Dateien und Screenshots als Beweismittel ab und ließen die daraus gewonnenen Erkenntnisse bei der Urteilsfindung außen vor. Die übrigen Vorwürfe des Arbeitgebers und die in der Stellungnahme des Arbeitnehmers eingeräumten Hinweise rechtfertigten für sich keine Kündigung ohne vorherige Abmahnung, sodass die Kündigung für unwirksam befunden wurde.

3 Parallelen zu bisheriger Rechtsprechung

Es ist alles andere als überraschend, dass die aus einer heimlichen Überwachung des Arbeitnehmers gewonnen Daten nicht verwertbar sind. Denn wertungsmäßig steht die Keylogging-Überwachung der verdeckten Videoüberwachung gleich (Stoffels 2017). Auch in diesem Zusammenhang wurde die Verwertbarkeit der personenbezogenen Daten und Erkenntnisse bereits in einem Urteil aus 2013 abgelehnt (BAG 2013: Rn. 49 ff.). Geklagt hatte damals eine Kassiererin, die im Verdacht stand, Geldbeträge aus dem Kassenbestand entnommen zu haben. Die Bestimmung des § 32 Abs. 1 S. 2 BDSG lässt eine personenbezogene Datenerhebung nur zur Aufdeckung von Straftaten zu, soweit der Eingriff erforderlich ist und dem Arbeitnehmer kein überwiegendes, schützenswertes Interesse zukommt. Hier muss das Interesse an der Verwertung der Videoaufnahmen mit dem Interesse der überwachten Person an ihrer informationellen Selbstbestimmung abgewogen werden. Die verdeckte Videoüberwachung setzt insofern einen konkreten Verdacht einer Straftat oder einer schweren Pflichtverletzung des Arbeitnehmers voraus und ist nur zulässig, sofern andere Mittel bereits ergebnislos ausgeschöpft wurden (BAG 2013: Rn. 50). Auch hier konnte der Arbeitgeber nicht nachweisen, dass falsche Abrechnungen zuvor konkret auf das Verhalten der gekündigten Kassiererin zurückzuführen waren. Die dargestellten Grundsätze für eine heimliche Aufzeichnung am Arbeitsplatz wurden auch für die heimliche Überwachung durch Keylogger angewandt und bestätigen, dass an die Zulässigkeit einer heimlichen Überwachung vor dem Hintergrund der Grundrechte des Arbeitnehmers hohe Anforderungen gestellt werden.

4 Rückenwind aus Straßburg

Auch der Europäische Gerichtshof für Menschenrechte stärkte in seinem kürzlich ergangenen Urteil (EGMR 2017) die Arbeitnehmerrechte. Ein Unternehmen hatte den Chat-Verlauf eines rumänischen Arbeitnehmers, der auf seinem Dienst-PC einen Messengerdienst nutzte, umfangreich aufgezeichnet. Auch Privatgespräche mit seinem Bruder und seiner Verlobten befanden sich unter den Aufzeichnungen. Aufgrund übermäßig privater Nutzung wurde ihm gekündigt. Nachdem er vor rumänischen Gerichten mit seiner Klage auf Weiterbeschäftigung scheiterte, entschied der Europäische Gerichtshof für Menschenrechte, dass diese Überwachung eines Dienst-Computers gegen das Recht auf Privatleben aus Art. 8 der Europäischen Menschenrechtskonvention verstößt und die Beweismittel aus diesem Grund nicht für die Begründung einer Kündigung genutzt werden dürfen.

5 Einordnung nach neuem Datenschutzrecht

Fraglich ist, ob das Urteil des Bundesarbeitsgerichts Bestand haben wird. Denn ab dem 25. Mai 2018 gilt in allen Mitgliedstaaten der EU die neue EU-Datenschutzgrundverordnung (DS-GVO). Diese enthält selbst zwar keine spezifischen Regeln zum Arbeitnehmerdatenschutz. Durch eine Öffnungsklausel in Art. 88 DS-GVO wird den Mitgliedstaaten aber ermöglicht, eine detaillierte Ausgestaltung für die Verarbeitung personenbezogener Beschäftigtendaten vorzunehmen. Dabei kann dieser Themenkomplex sowohl gesetzlich als auch durch Tarifverträge oder Betriebsvereinbarungen geregelt werden.

Mit der Neuregelung des Arbeitnehmerdatenschutzes in § 26 BDSG-neu ist der deutsche Gesetzgeber diesem Auftrag nachgekommen. Personenbezogene Daten

von Beschäftigten dürfen demnach nur verarbeitet werden, sofern dies für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Dies ist durch eine Verhältnismäßigkeitsabwägung zwischen den widerstreitenden Interessen von Arbeitgeber und Arbeitnehmer zu ermitteln. Zur Aufdeckung von Straftaten müssen darüber hinaus dokumentierte, tatsächliche Anhaltspunkte einen Verdacht begründen. Dies entspricht im Wesentlichen der bereits bestehenden Regelung des § 32 BDSG, sodass die Rechtsprechung Bestand haben wird.

Der heimliche Einsatz von Keyloggern oder anderen Überwachungs-Tools kann demnach auch zukünftig nicht auf diesen gesetzlichen Erlaubnistatbestand gestützt werden. Möglich ist es aber, die Überwachung offenzulegen und dahingehend eine Betriebsvereinbarung mit dem Betriebsrat abzuschließen oder eine Einwilligung einzuholen. Insbesondere für die Einwilligung ergeben sich jedoch hohe Anforderungen: Eine solche ist nur wirksam, wenn der Arbeitnehmer freiwillig entscheiden durfte, § 26 Abs. 2 BDSG-neu. Wegen des Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer ist dies im Einzelfall genau zu prüfen. Angenommen wird die Freiwilligkeit z.B. wenn die Einwilligung zu einem wirtschaftlichen oder rechtlichen Vorteil für den Arbeitnehmer führt, Erwägungsgrund 155. Dies wird jedoch oft nicht der Fall sein, sodass auch die Möglichkeit, eine Einwilligung einzuholen, keine Rechtssicherheit für den Arbeitgeber verspricht.

6 Keylogger auch Thema im US-amerikanischen Recht

Auch in den USA ist Keylogging am Arbeitsplatz bereits Gegenstand von Gesetzgebung und Rechtsprechung gewesen. Der US-amerikanische „Federal Wiretap Act" verbietet jedes absichtliche Abfangen von mündlichen, kabelgebundenen und elektronischen Kommunikationsdaten.[1] Abfangen meint dabei die akustische oder in sonstiger Weise durchgeführte Beschaffung elektronischer, kabelgebundener oder mündlicher Kommunikationsinhalte unter Einsatz elektronischer, mechanischer oder anderer Geräte. In einem ähnlichen Fall hat der Beklagte ebenfalls einen Keylogger auf dem Computer seines Mitarbeiters installiert und sich die Daten übermitteln lassen.[2] Ein kalifornisches Gericht entschied, dass ein Gerät oder Programm, das Kommunikationsdaten innerhalb eines Nutzersystems aufzeichnet, kein „Abfangen" im Sinne des Gesetzes darstelle (Bellia 2005: 1304). Das US-amerikanische Gesetz reguliert danach gerade einige besonders gefährliche Spyware-Softwares – insbesondere die Keylogger-Software – nicht (Bellia 2005: 1304). Eine höchstrichterliche Rechtsprechung dazu ist bislang nicht ergangen. Dennoch lässt sich auch hier erkennen, dass der Datenschutz auf nationaler und europäischer Ebene deutlich weitgehender ausgestaltet ist und umfassender schützt als in den Vereinigten Staaten.

7 Fazit

Vermehrt ergeben sich Anwendungszenarien für Big Data in den Personalabteilungen der Unternehmen. Die datenschutzrechtlichen Grenzen, die dabei zu beachten sind, wurden allerdings kürzlich vom Bundesarbeitsgericht betont. So ist der heimliche Einsatz von Keyloggern zur Datengewinnung unzulässig. Dadurch wurden die Persönlichkeitsrechte von Arbeitnehmern gestärkt. Dies findet auch auf europäischer Ebene Resonanz – sowohl, wie ebenfalls kürzlich entschieden, nach der europäischen Menschenrechtskonvention, als auch nach dem zukünftig anwendbaren Regime der europäischen DS-GVO. So ist davon auszugehen, dass europäische datenverarbeitende Unternehmer – im Gegensatz zu ihren amerikanischen Kollegen – auch künftig Einwilligungen der Arbeitnehmer einholen müssen oder Betriebsvereinbarungen mit den Arbeitnehmervertretungen abschließen müssen, wenn sie Daten

[1] § 2511(1)(a) Federal Wiretap Act.

[2] US v. Ropp 347 F. Supp. 2d 831 (C.D. Cal. 2004).

von Arbeitnehmern oder Bewerbern zu HR-Zwecken umfangreich auswerten wollen.

Literaturnachweise

Bellia, P. (2005). Sypware and the Limits of Surveillance Law, *Berkeley Technology Law Journal, Vol. 20*, 1283-1343.

Bundesarbeitsgericht (2013). Urteil vom 21.11.2013. Az.: 2 AZR 797/11. BeckRS 2014, 66050.

Bundesarbeitsgericht (2017). Pressemitteilung Nr. 31/17. Online verfügbar unter http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&nr=19403.

Bundesarbeitsgericht (2017). Urteil vom 27. Juli 2017. Az.: 2 AZR 681/16.

Ciampa, M. (2017). Security Awareness – Applying Practical Security in your World, 5. Auflage. Boston: Cingage Learning.

Europäischer Gerichtshof für Menschenrechte (2017). Case of Bărbulescu v. Romania. Application No. 61496/08. Online verfügbar unter: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}

Landesarbeitsgericht Hamm (2016). Urteil vom 17.6.2016. Az.: 16 Sa 1711/15. BeckRS 2016, 72746.

Springer Gabler Verlag (Hrsg.) (2017). Gabler Wirtschaftslexikon, Stichwort: Keylogger. Online verfügbar unter: http://wirtschaftslexikon.gabler.de/Archiv/1408525/keylogger-v3.html.

Stoffels, M. (2017). BAG zur Überwachung mittels Keylogger (Kommentar). Online verfügbar unter https://community.beck.de/2017/07/28/bag-zur-ueberwachung-mittels-keylogger.

Vogelsang, S. & Hesser, S. & Möllers, F. (2016). Hardware-Keylogger. Die Tastatur in der Hand des Feindes. *DuD 2016*, 729-734.

ABIDA (Assessing Big Data) Über die Dossiers

Das Projekt ABIDA, gefördert vom Bundesministerium für Bildung und Forschung (Förderkennzeichen 01IS15016A-F), lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung. In den Dossiers werden regelmäßig ausgewählte Big Data-Themen kurz und prägnant dargestellt, um dem Leser einen Überblick zu liefern und einen Einstieg in die Thematik zu ermöglichen. Weitere Dossiers sind verfügbar unter www.abida.de/content/dossiers.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Vertiefungshinweise: Literatur und Links

- **Tiedemann, J. (2017).** LAG Hamm: Heimlicher Einsatz eines Keyloggers am Arbeitsplatz. *ZD 2017*, 140-143.
- **Europäischer Gerichtshof für Menschenrechte (2017).** Case of Bărbulescu v. Romania. Application No. 61496/08. Online verfügbar unter: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}