

## Fallbeispiele zum IT-Recht – Arbeitnehmerüberwachung per Keylogger

Durch die heutigen technischen Möglichkeiten ist es für den Arbeitgeber ohne weiteres möglich die Arbeitnehmer nahezu lückenlos zu überwachen. Insbesondere bei PC-Arbeitsplätzen kann durch Softwareunterstützung alles bis auf den Tastaturanschlag überwacht und gespeichert werden.

Aber ist das auch wirksam? Was darf der Arbeitgeber hier bzw. wie weit reichen die Rechte des Arbeitnehmers in diesen Fällen?

In unserem Fallbeispiel heute geht es um genau diese Frage. Die Antwort basiert auf den gekürzten und vereinfachten Entscheidungsgründen des Bundesarbeitsgerichts (BAG). Bitte lesen Sie zunächst nur das Fallbeispiel und die Frage und versuchen Sie selbst Ihr Rechtsempfinden zu befragen, bevor Sie sich die Lösung ansehen.

### Fallbeispiel:

Die Parteien streiten über die Wirksamkeit einer außerordentlichen, hilfsweise ordentlichen Kündigung. Der Kl. war bei der Bekl., die in ihrem Betrieb regelmäßig mehr als zehn Arbeitnehmer beschäftigt, seit Juli 2011 als Webentwickler tätig. Zu Beginn des Arbeitsverhältnisses verpflichtete er sich schriftlich, Hard- und Software aus Gründen der informationstechnischen Sicherheit ausschließlich zur Erfüllung der vereinbarten Aufgaben zu nutzen. Im Zusammenhang mit der Anbindung eines neuen Netzwerks richtete die Bekl. am 19.4.2015 (Sonntag) eine E-Mail folgenden Inhalts an ihre Mitarbeiter:

*„Hallo liebes (...) Team,  
es ist soweit, die Telekom hat es endlich geschafft, uns einen schnellen Internet Anschluss bereitzustellen. Dieses möchte ich Euch natürlich nicht vorenthalten, aus diesem Grund erhaltet Ihr freien Zugang zum WLAN.  
Da bei Missbrauch, zum Beispiel Download von illegalen Filmen, etc. der Betreiber zur Verantwortung gezogen wird, muss der Traffic mitgelogged werden. Da ein rechtlicher Missbrauch natürlich dann auch auf denjenigen zurückfallen soll, der verantwortlich dafür war.  
Somit:  
Hiermit informiere ich Euch offiziell, dass sämtlicher Internet Traffic und die Benutzung der Systeme [der Bekl.] mitgelogged und dauerhaft gespeichert wird. Solltet Ihr damit nicht einverstanden sein, bitte ich Euch mir dieses innerhalb dieser Woche mitzuteilen.  
Bitte benutzt dieses Netzwerk für alles wie Spotify, YouTube, etc. um unser Hauptnetzwerk zu entlasten. (...)“*

In einer Unterweisung am 20.4.2015 wandte sich kein Arbeitnehmer gegen die Absicht der Bekl., den „Internettraffic“ und die Benutzung ihrer Systeme zur Verhinderung von Missbrauch des Internetzugangs „mitzuloggen“.

Die Bekl. installierte sodann auf dem Dienst-PC des Kl. eine Software, die ab dem 21.4.2015 alle Tastatureingaben protokollierte und regelmäßig Screenshots fertigte (Keylogger). Nachdem die Bekl. die vom Keylogger erstellten Dateien ausgewertet hatte, fand am 4.5.2015 ein Gespräch mit dem Kl. statt, in dem dieser einräumte, seinen Dienst-Rechner während der Arbeitszeit privat genutzt zu haben. Er gab an, ein Computerspiel programmiert und E-Mail-Verkehr für das Logistikunternehmen seines Vaters abgewickelt zu haben. Auf die Programmierung des Spiels habe er am Arbeitsplatz in der Zeit von Januar bis April 2015 ca. drei Stunden verwendet. Für die Firma seines Vaters sei er – vorwiegend in seiner Freizeit – höchstens etwa zehn Minuten täglich tätig gewesen. Die Bekl. kündigte das Arbeitsverhältnis des Kl. daraufhin mit Schreiben vom 19.5.2015 außerordentlich fristlos, hilfsweise ordentlich zum nächstzulässigen Termin.

Hiergegen hat sich der Kl. fristgerecht mit der vorliegenden Klage gewandt. Er hat behauptet, die privaten Verrichtungen meist in den Pausen und in Zeiten erledigt zu haben, in denen er keines der ihm zugewiesenen Projekte habe bearbeiten können. Die Bekl. habe durch den Einsatz eines Keyloggers „hinterrücks“ und ohne jeden Anlass massiv in sein Grundrecht auf informationelle Selbstbestimmung eingegriffen. Die Bekl. hat beantragt, die Klage abzuweisen. Aus den vom Keylogger erstellten Dateien ergebe sich, dass der Kl. am 21.4.2015 weitaus länger mit der Entwicklung des Computerspiels beschäftigt gewesen sei, als er eingeräumt habe. Die Einträge in den Logdateien widerlegten zudem seine Behauptung, höchstens zehn Minuten täglich mit Aufgaben für die Firma seines Vaters befasst gewesen zu sein.

## FRAGE:

Ist die außerordentliche Kündigung der Bekl. wirksam?  
Ist zumindest die ordentliche Kündigung der Bekl. wirksam?

## ANTWORT:

### **NEIN und NEIN.**

Die Kündigungen der Bekl. vom 19.5.2015 sind unwirksam. Es fehlt sowohl an einem wichtigen Grund für die außerordentliche Kündigung (§ 626 I BGB) als auch an einer sozialen Rechtfertigung für die unter Geltung des Kündigungsschutzgesetzes (§§ 1 I, 23 I) erklärte ordentliche Kündigung (§ 1 II KSchG) (...).

Bei der Entscheidung muss der Sachvortrag der Bekl. unberücksichtigt gelassen werden, den sie nur aufgrund des von ihr eingesetzten Keyloggers in das Verfahren einführen konnte. Die Verwertung dieses Vorbringens bei der Urteilsfindung wäre mit dem Recht des Kl. auf informationelle Selbstbestimmung unvereinbar. Es besteht also ein Sachvortrags- oder Beweisverwertungsverbot wegen einer Verletzung des allgemeinen Persönlichkeitsrechts des Kl.

Die Datenerhebung durch den Keylogger griff in das Recht des Kl. auf informationelle Selbstbestimmung ein. Der Kl. hat in die Maßnahme nicht eingewilligt. Der Eingriff war nicht aufgrund überwiegender Interessen der Bekl. gerechtfertigt. Ebenso lagen keine weiteren, über das schlichte Beweisinteresse der Bekl. hinausgehenden Aspekte vor, die gerade die infrage stehende verdeckte Informationsbeschaffung durch einen Keylogger als gerechtfertigt erscheinen lassen könnten.

Die Aufzeichnung und Speicherung der Tastatureingaben am Dienst-PC des Kl. sowie das Fertigen von Screenshots durch den Keylogger stellten Datenerhebungen dar. Der Kl. hat in die Datenerhebungen nicht dadurch eingewilligt, dass er der Ankündigung der Bekl. nicht widersprochen hat. Allein in der Tatsache, dass ein Arbeitnehmer einer ihm mitgeteilten Maßnahme nicht entgegentritt, liegt keine Einverständniserklärung in die Informationserhebung. Das Unterlassen eines Protests kann nicht mit einer Einwilligung gleichgesetzt werden. Das gilt insbesondere, wenn – wie vorliegend – eine vom Arbeitgeber gesetzte „Widerspruchsfrist“ noch nicht abgelaufen ist. Im Übrigen hatte die Bekl. dem Kl. nicht eröffnet, es sollten alle Tastatureingaben an seinem Dienst-PC „mitgeloggt“ und regelmäßig Screenshots gefertigt werden. Auch konnte der Kl. nicht erkennen, zu welchem Zweck er überwacht wurde. Die E-Mail der Bekl. vom 19.4.2015 legte den Schluss nahe, dass allein eine etwaige Internetaktivität über das neue Netzwerk und diese auch „nur“ hinsichtlich der abgerufenen Inhalte („Download von illegalen Filmen“, „Betreiber zur Verantwortung gezogen“, „rechtlicher Missbrauch“) kontrolliert werden sollte.

Mit der ohne Einwilligung des Kl. erfolgten Datenerhebung durch den Keylogger hat die Bekl. in dessen geschütztes Recht auf informationelle Selbstbestimmung eingegriffen. Für einen Eingriff

in den Schutzbereich dieses Grundrechts ist es ohne Bedeutung, ob die Datenerhebung in verdeckter Form oder für den Arbeitnehmer erkennbar erfolgt.

Bei dem verdeckten Einsatz eines Keyloggers wird der betroffene Arbeitnehmer in der Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden, beschränkt, indem er zum Ziel einer nicht erkennbaren – systematischen – Beobachtung durch den Arbeitgeber gemacht wird und dadurch auf sich beziehbare Daten über sein Verhalten preisgibt, ohne die Überwachung oder gar den mit ihr verfolgten Verwendungszweck zu kennen.

Wird der Keylogger offen eingesetzt, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, weil die Aufzeichnung und Speicherung sämtlicher Tastatureingaben und bestimmter Bildschirminhalte der Vorbereitung möglicher belastender Maßnahmen (Ermahnung, Abmahnung, Kündigung) dienen und zugleich abschreckend wirken und insoweit das Verhalten des Betroffenen lenken soll.

Der Einsatz des Keyloggers war der Bekl. nicht erlaubt. Es fehlte bereits an dem insoweit erforderlichen, durch konkrete Tatsachen begründeten Anfangsverdacht einer Straftat oder einer anderen schweren Pflichtverletzung. Eine Maßnahme, die hinsichtlich der Intensität des durch sie bewirkten Eingriffs in das allgemeine Persönlichkeitsrecht des Arbeitnehmers mit einer (verdeckten) Videoüberwachung vergleichbar ist, stellt sich als unverhältnismäßig dar, wenn sie aufgrund bloßer Mutmaßungen ergriffen wird.

*(BAG, Urteil vom 27.7.2017, Aktenzeichen 2 AZR 681/16)*

## **Fazit**

Der Einsatz eines Keyloggers stellt also grundsätzlich eine Verletzung des grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung des Arbeitnehmers dar.

Nur unter ganz bestimmten Umständen, die einer eingehenden Abwägung bedürfen, ist es dem Arbeitgeber ausnahmsweise erlaubt dennoch eine solche Maßnahme durchzuführen. Das BAG nimmt dabei Bezug auf die hohen Hürden der verdeckten Videoüberwachung von Arbeitnehmern, die nur bei konkretem Verdacht auf Begehung einer Straftat erlaubt ist.

Ist der Einsatz des Keyloggers weder durch eine wirksame Einwilligung des Arbeitnehmers gedeckt (bloßes Schweigen ist keine solche Einwilligung), noch durch die Vorschriften des Datenschutzrechts oder sonstige, über das schlichte Beweisinteresse hinausgehende Aspekte gerechtfertigt, löst dies ohne weiteres ein Beweisverwertungsverbot aus. Der Arbeitgeber darf also keiner der so gewonnenen Informationen in einem Verfahren für sich verwerten. Diese Informationen müssen unberücksichtigt bleiben.

Daher war vorliegend auch die Kündigung als unwirksam zurückzuweisen.

Timo Schutt  
Rechtsanwalt  
Fachanwalt für IT-Recht

[www.schutt-waetke.de](http://www.schutt-waetke.de)  
[ra-schutt@schutt-waetke.de](mailto:ra-schutt@schutt-waetke.de)