

Achtung, der Chef lauscht mit!

Verdacht Der Anspruch eines Arbeitgebers auf Qualität und Effizienz bei der Arbeit ist legitim. Doch überschreitet ein Chef mit manchen Überwachungsmaßnahmen seine Kompetenzen? Marie-Louise Gächter, Leiterin der Datenschutzstelle in Liechtenstein, gibt Auskunft.

Vertrauen ist gut, Kontrolle ist besser, lückenlose Überwachung am besten, denkt sich mancher Arbeitgeber. Wie weit darf ein Chef gehen, ohne seine Kompetenzen gegenüber seinen Mitarbeitenden zu überschreiten?

Ein Liechtensteiner Arbeitgeber hegt den Verdacht, dass seine Angestellten während der Arbeitszeit vorwiegend privaten Interessen im Internet nachgehen. Um aus Verdachtsmomenten Tatsachen zu schaffen, installiert er fortan überall im Betrieb Kameras, die das Arbeitsverhalten der Angestellten aufzeichnen. Ist das nun erlaubt?

Grundfreiheiten berücksichtigen

Marie-Louise Gächter, Leiterin der nationalen Datenschutzstelle in Liechtenstein, erklärt, der Arbeitgeber könne sich grundsätzlich auf seine «berechtigten Interessen» stützen, müsse allerdings abwägen, ob nicht die Grundfreiheiten der Arbeitnehmer gefährdet seien. Beispielsweise sei ein solch tiefgreifender Eingriff gegeben, wenn der Mitarbeitende permanent gefilmt werde, etwa die Bankangestellte am Arbeitsplatz. Auch die Überwachung eines Pausenraums, der Cafeteria, der Raucherecke oder einer Umkleidekabine sei als tiefgreifender Eingriff in die Grundrechte der Betroffenen qualifiziert. Zur Aufdeckung von Straftaten dürften Aufnahmen von Beschäftigten nur dann gemacht werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen habe.

Und selbst das Schnüffeln des Arbeitgebers in den Mails seiner Angestellten ist grundsätzlich untersagt. «Eine Notwendigkeit zur umfassenden und permanenten Einsicht in den personalisierten Email-Account kann nicht abgeleitet werden. Was die Ausnahmefälle betrifft, kann ein solcher dann angenommen werden, wenn etwa ein konkreter Verdacht besteht für ein rechtswidriges Verhalten des Arbeitnehmers», so Gächter. In jedem



Lückenlose Videoüberwachung am Arbeitsplatz: Dem Arbeitgeber sind in Liechtenstein Grenzen gesetzt. Bild iStock.

Fälle seien aber auch hier die Persönlichkeitsrechte des Mitarbeitenden zu achten, indem etwa private Mails eingesehen würden, sondern nur geschäftliche. Ebensovien dürfe der Verdachtsfall zu einer Totalüberwachung führen.

Aufzeichnung bei Ausnahmen

Beim Ausforschen der Telefongespräche sei zu differenzieren: Zum einen gebe es eine gesetzliche Ver-

pflichtung zum Aufzeichnen von Telefongesprächen, wie in der Verordnung vom 22. Februar 1994 über die Banken und Wertpapierfirmen festgelegt wurde. Zum anderen könne eine Aufzeichnung von Telefongesprächen mit Einwilligung des externen Gesprächspartners zulässig sein. Das gelte auch für einen Mitarbeitenden. Nur in Ausnahme- oder Einzelfällen könne eine Aufzeichnung ohne seine Einwilligung stattfinden, wenn konkrete Beschwer-

den von Kunden vorliegen oder es klare Anhaltspunkte für Qualitätsmängel gebe.

Mitarbeitern ist oft nicht klar, wie weit der Chef bei der Überwachung und Datensammlung gehen darf. Das Thema sei ein Dauerbrenner, wie Marie-Louise Gächter zu berichten weiss: «Wir haben bereits einige Fragen zu dieser Thematik erhalten, sowohl von Arbeitgebern als auch Arbeitnehmern. Auch bei unseren Informati-

onsveranstaltungen ist dies immer wieder ein Thema.» Die Fragenden arbeiten in ganz unterschiedlichen Branchen. Insgesamt lasse sich aber sagen, dass die Tendenz zur Überwachung dort am höchsten sei, wo es um sensible Bereiche gehe oder der Arbeitgeber ein besonders grosses Interesse habe, sicherzustellen, dass Mitarbeitende ihre Tätigkeit korrekt und nicht rechtswidrig ausübten.

Wird «1984» Realität?

Im Ausland bahnen sich an einigen Orten totalitäre Überwachungsformen an: Die US-Firma Three Square Market sorgte 2017 für einen weltweiten Aufschrei, weil sie die Mitarbeiter zu einer sogenannten «Chip-Party» einlud. Dabei liessen sich die Mitarbeiter freiwillig einen reiskorngrossen Chip unter die Haut implantieren, mit dem fortan Türen geöffnet, in der Kantine bezahlt oder der Computer entsperrt werden konnte. Fünfzig Personen sollen sich damals freiwillig gemeldet haben, in der Zwischenzeit dürften es bereits wesentlich mehr sein, die den Schlüsselerersatz nutzen. Auch in Schweden wird diese Technik seit längerem verwendet: Vorreiter war 2015 das schwedische Start-up Epicenter.

Die Aufrüstung zum Cyborg hört sich bequem an, birgt jedoch immense Gefahren. Denn mit Mikrochips lässt sich prinzipiell eine lückenlose Überwachung der Arbeiter realisieren. Die Privatsphäre verschwindet. Derart dystopisch sieht Marie-Louise Gächter, Leiterin der nationalen Datenschutzstelle in Liechtenstein, die Zukunft jedoch nicht: «Auf den Arbeitsplatz bezogen droht in Zukunft keine komplette Überwachung. Das heisst nicht, dass es keine Tendenzen in die Richtung gibt, sondern dass die gesetzlichen Voraussetzungen dagegen sprechen. Ein Arbeitgeber muss sehr gründlich prüfen und abwägen, ob die Überwachung erforderlich und rechtlich zulässig ist.» Die Auswirkungen lückenloser Überwachung zeigte George Orwell in seiner Dystopie «1984». Es ist erstaunlich, dass sich heute Arbeiter freiwillig der Kontrolle unterwerfen.

«Big Brother Awards» rütteln Schweizer wach

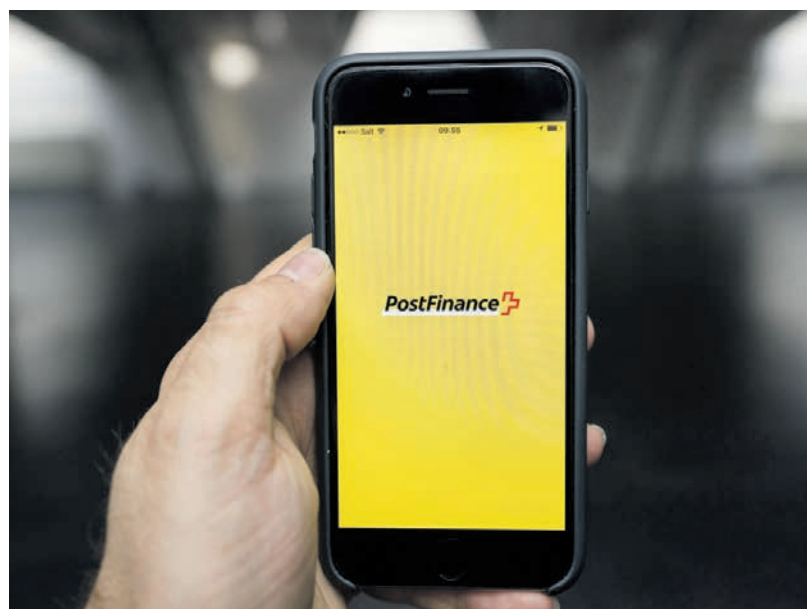
Datenklau Am Donnerstag wurden an der Universität Zürich die grössten Datenkraken der Schweiz mit einem Schmähprijs ausgezeichnet. Traurige Gewinner sind Postfinance, das elektronische Patientendossier (EPD) und die «Geheimjustiz»-Abteilung im Kanton Zürich.

VON RETO MÜNDLE

Überwachung findet heutzutage längst nicht mehr ausschliesslich am Arbeitsplatz statt. Die Daten über unser tagtägliches Verhalten werden mitgeschnitten, gesammelt und ausgewertet: Informationen darüber, was uns interessiert, wohin wir gehen, was wir kaufen, wie wir leben, wie gesund oder krank wir sind, mit wem wir kommunizieren oder was wir tun. Die technischen Möglichkeiten dafür wachsen schnell, die Gesetzgebung hechelt hinterher.

Für die funktionierende Demokratie

In Zürich wurden am Donnerstag nach zehnjährigem Unterbruch wieder die sogenannten «Big Brother Awards» verliehen. Mit der Preisverleihung werden die schlimmsten «Datenkraken» aus Privatwirtschaft und Politik ans Licht der Öffentlichkeit gezerrt. Das Organisations-team und die Schweizer Jury rekrutieren sich aus den gemeinnützigen und unabhängigen Organisationen Chaos Computer Club Schweiz, Digitale Gesellschaft und die p=π Stiftung. Ziel ist es, über konkrete Fälle zu informieren. Darüber hinaus erhoffen sich die Initianten aber vor allem auch, dass der Gesetzgeber sich der Problematik bewusst wird und entsprechend handelt. Denn: Fairness, Ausgewogenheit und Selbstbestimmung bil-



Die Postfinance speichert Stimmabdrücke ihrer Kunden.

Bild: keystone

den die Grundlage für eine funktionierende Demokratie. Nach der Vorstellung der Jury sowie der Eröffnungsrede durch Gabriele Siegert, der Vize-Rektorin der Universität Zürich, wurden die Sieger prämiert, die in drei Kategorien ermittelt wurden: «Publikum», «Private-Public-Partnership» sowie «Staat». Die Postfinance erhielt den «Publikums»-Preis, weil sie seit September 2018 den Stimm-

abdruck verwendet, um die Kunden am Telefon zu identifizieren. Die Stimmerkennung ist grundsätzlich aktiviert. Die Kunden müssen die Stimmerkennung deaktivieren, also explizit widersprechen, wenn sie nicht wollen, dass von ihrer Stimme ein Abdruck gemacht und gespeichert wird. Bei einem Stimmabdruck handelt es sich um ein sehr persönliches, biometrisches Datum, vergleichbar mit

einem Fingerabdruck. Es ist damit möglich, einen Menschen auch in anderen Kontexten zu überwachen. Sogar ein Identitätsdiebstahl ist grundsätzlich möglich.

Zentralismus als Datenklau-Gefahr

In der Kategorie «Private-Public-Partnership» wurde das Elektronische Patientendossier (EPD) ausgezeichnet. Gesundheitsdaten sind besonders schützenswerte Personendaten und zudem potenziell hochdiskriminierend. Sie sind kaum oder nicht veränderlich und haften einer Person lange oder lebenslanglich an. Patientendaten werden aktuell dezentral in den Systemen der Ärzte und Spitäler gehalten, allerdings im Einzelfall unter zum Teil katastrophalen Sicherheitsstandards. Die Systeme sind allerdings jeweils unterschiedlich gestrickt und angebunden, sodass ein möglicher Datendieb unterschiedliche Angriffe ausführen muss, um viele Patientendaten einzusammeln. Mit einem dezentralisierten und sicher geführten EPD könnte dieser Missstand behoben werden. Stattdessen wird offenkundig an einem EPD gearbeitet, das technisch zentralistisch und von nur zwei Systemanbietern (Swisscom und Post) betrieben wird. Damit entstehen zentralisierte Angriffspunkte. Das gilt im selben Masse auch für Liechtenstein, das sich im Frühjahr 2016 für den Systemanbieter Swisscom

Health AG entschieden hat, wie im Vernehmlassungsbericht der Regierung betreffend die Schaffung eines Gesetzes über das elektronische Gesundheitsdossier geschrieben steht.

Überwachungsstaat Schweiz?

In der Kategorie «Staat» wurde das Zwangsmassnahmengericht im Kanton Zürich angeprangert: Zwangsmassnahmengerichte sind für die Bewilligung von Zwangsmassnahmen im Rahmen von Strafuntersuchungen zuständig: Sie beurteilen, ob schwere Grundrechtseingriffe wie Untersuchungshaft, Telefonüberwachung, Verwanzung von Wohnungen angewendet werden dürfen. Bei (geheimen) Überwachungsmaßnahmen müssen sie sich in ihrem Urteil auf die Aussagen der Untersuchungsbehörden verlassen, da natürlich die verteidigende Partei nicht angehört werden kann. In der Praxis winken die Gerichte mit 97 Prozent fast alle Anträge durch. Diese Praxis wurde speziell im Zusammenhang mit Staatstrojanern durch die Kantons-polizei Zürich scharf kritisiert: Die Trojaner sind geeignet, die digitale Intimsphäre zu verletzen, da sich auf dem Computer und den Handys unzählige hochsensible Daten anhäufen: Fotos und Videos, Adresslisten und Kalendereinträge, Korrespondenz per E-Mail oder SMS, Passwörter, Kontoverbindungen und Gesundheitsdaten.