Deutscher Bundestag **Drucksache 19/12552**

19. Wahlperiode 21.08.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/12182 –

Überwachung von Mitarbeitern durch Diensthandys und andere PC-Tools im Spannungsverhältnis zum Datenschutz

Vorbemerkung der Fragesteller

Nach der Wahrnehmung der Fragesteller sind Installationen von Überwachungstechnologie im öffentlichen Raum ein gewohntes Bild und begleiten nicht nur Ausnahme- sondern lebensalltägliche Situationen eines Bürgers: Kameras finden sich auf Flughäfen, in Bankfilialen, auf Bahnhöfen, vor Geldautomaten, in U-Bahn-Stationen, in öffentlichen Gebäuden und vielen anderen Bereichen des öffentlichen Lebens. Doch die Überwachungstechnik macht auch nicht vor den eigenen vier Wänden halt. Spätestens seit der Markteinführung von so genannten Smart Speakern und sprachgesteuerten, internetbasierten intelligenten persönlichen Assistenten wie „Alexa“ hören immer öfter Unberechtigte mit (www.smartdroid.de/assistant-google-mitarbeiter-hoeren-mit-was-nicht-weiter-ueberrascht/).

Die technischen und digitalen Überwachungsmöglichkeiten beschränken sich allerdings nicht nur auf öffentliche Plätze und die Wohnung, sondern greifen schon längst auch auf den Arbeitsplatz über. Deutsche Unternehmen scheinen leider hier keine Ausnahme darzustellen.

Ein dienstlich genutztes Smartphone oder die Navigationssoftware im Dienstauto können dem Arbeitgeber eine Fülle von Daten übermitteln. Das kann dazu führen, dass der Arbeitgeber mehr Informationen zur Verfügung hat, als jemals zuvor. Zum einen kann die Überwachung von Arbeitsplätzen durchaus zweckmäßig im Sinne von Arbeitsabläufen und zur Verhinderung von Straftaten beitragen, allerdings wird in letzter Zeit vermehrt auf die Überwachung von Mitarbeitern gesetzt (www.manager-magazin.de/premium/ueberwachung-audiostory-sie-kennen-dich-sie-kriegen-dich-a-93348364-075b-4793-bc9a-452d89b21d74).

Mitarbeiter, die softwaregestützte Technologien nutzen, um beispielsweise Ein- und Ausgänge oder Login-Verhalten zu kontrollieren, haben die Möglichkeit, detaillierte Mitarbeiterprofile zu erstellen.

Die Überwachungsskandale wie die der Deutschen Telekom AG (www.manager-magazin.de/unternehmen/artikel/a-555158.html), der Deutschen Bahn AG (www.zeit.de/online/2009/04/bahn-bespitzelung) oder des Lebensmittel-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 19. August 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

konzerns Lidl (www.stern.de/wirtschaft/news/ueberwachungsskandal-lidl-muss-millionen-strafe-zahlen-3762026.html) haben offenbar ihre abschreckende Wirkung verloren. In Unternehmen in den USA und Großbritannien werden E-Mails, Web-Browser, Chatprogramme, Anrufbeantworter aber auch soziale Netzwerke überwacht (www.manager-magazin.de/premium/ueberwachung-audiostory-sie-kennen-dich-sie-kriegen-dich-a-93348364-075b-4793-bc9a-452d89b21d74).

In Deutschland ist so eine Praxis der Arbeitgeber illegal, denn grundsätzlich dürfen keine Daten genutzt werden, bei deren Beschaffung das Grundrecht auf in-formationelle Selbstbestimmung gebrochen wird. Zudem kommen gemäß der Datenschutz-Grundverordnung (DSGVO) dem Arbeitgeber umfangreiche Aufklärungs- und Unterrichtungspflichten zu.

1. Sind die in der Vorbemerkung der Fragesteller formulierten Umstände der potentiellen und teils umgesetzten Überwachungsmöglichkeiten der Arbeitnehmer der Bundesregierung bekannt?

Der Bundesregierung sind die infolge des technischen Fortschritts auch im Hinblick auf die Kontrolle von Beschäftigten gesteigerten technischen Möglichkeiten bekannt. Hinsichtlich der Sicherheit einer Verarbeitung von personenbezogenen Daten auch von Beschäftigten sind u. a. die Anforderungen von Artikel 32 DSGVO zu beachten.

Für die Prüfung datenschutzrechtlicher Verstöße von Arbeitgebern gegenüber ihren Beschäftigten sind neben den betrieblichen Datenschutzbeauftragten im Einzelfall die unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern zuständig (Artikel 57 Absatz 1 DSGVO). Der Bundesregierung liegen insofern keine Erkenntnisse zu den aufsichtsbehördlichen Verfahren vor.

Erlaubt der Arbeitgeber die (auch) private Nutzung der betrieblichen Internet- und Telekommunikationsdienste wird er zudem zum Dienstanbieter im Sinne des Telekommunikationsgesetzes (TKG) bzw. Telemediengesetzes (TMG). Diese Gesetze sichern u. a. das Fernmeldegeheimnis ab und unterwerfen den Dienstanbieter bestimmten Vertraulichkeitsvorgaben und zwar nicht nur gegenüber den Beschäftigten, sondern auch im Hinblick auf die Kommunikation von Dritten (also Externen, die den Beschäftigen private Mails zurückschicken). Nach den Vorgaben des TKG und TMG darf der Arbeitgeber die Kommunikation nur in eng begrenzten Einzelfällen durchsuchen.

Insbesondere hat eine fehlende Trennung bzw. Unterscheidungsmöglichkeit von dienstlichen und privaten E-Mails zur Folge, dass dem Arbeitgeber der Zugriff auf die dienstliche Kommunikation des Beschäftigten versagt ist. Verstöße hiergegen können strafrechtliche Konsequenzen haben (u. a. § 206 StGB).

2. Sieht die Bundesregierung bei der Transformation der DSGVO in nationales Recht gesetzgeberischen Handlungsbedarf, dass die persönlichen Rechte der Arbeitnehmer besser zu schützen sind?

Die Bundesregierung verweist auf die Antworten zu Frage 15 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/8485 sowie zu Frage 6 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2653.

3. Ist der Bundesregierung bekannt, wie viele Fälle vor dem Bundesarbeitsgericht in Bezug auf „Lauschangriffe“ auf Mitarbeiter verhandelt wurden?

Der Bundesregierung liegen hierzu keine Daten vor. Eine Statistik im Sinne der Fragestellung wird beim Bundesarbeitsgericht nicht geführt.

4. Welche Maßnahmen hat die Bundesregierung umgesetzt, um Mitarbeiter des öffentlichen Dienstes vor solchen Übergriffen zu schützen?

Auf die Antwort zu Frage 2 wird verwiesen.

5. Wie beurteilen das Bundesamt für Sicherheit in der Informationstechnik und der Bundesdatenschutzbeauftragte den derzeitigen Stand des Mitarbeiterschutzes in den bundeseigenen Einrichtungen?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist nach § 3 Absatz 1 Satz 2 Nummer 1 BSIG zuständig für die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes. Die Frage nach dem Stand des Schutzes von Mitarbeiterinnen und Mitarbeitern der Bundesverwaltung erschöpft sich in der Bewertung datenschutzrechtlicher Fragen; hierfür ist das BSI nicht zuständig.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist nicht Teil der Bundesregierung und in seiner Aufgabenerledigung und Meinungsfindung völlig unabhängig (§ 10 Absatz 1 BDSG). Die Bundesregierung nimmt nicht für den BfDI Stellung.

6. Wie beurteilt der Bundesdatenschutzbeauftragte die Software Windows 10 in Bezug auf Sicherheit und Abhörsicherheit und deren Implementierung in der öffentlichen-rechtlichen Dienstbenutzung?

Die Bundesregierung kann für den unabhängigen Beauftragten für den Datenschutz und die Informationsfreiheit keine Stellungnahme abgeben. Insofern wird auf den zweiten Teil der Antwort zu Frage 5 verwiesen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333