B u c h r e z e n s i o n

Jörg Eisele, Compliance und Datenschutzstrafrecht, Strafrechtliche Grenzen der Arbeitnehmerüberwachung, Nomos Verlagsgesellschaft, Baden-Baden 2012, 116 S., € 29,-

Die Enthüllungen des US-Whistleblowers Edward Snowden in der „NSA-Affäre" machten nachhaltig deutlich, auf welchen brüchigen Fundamenten der Datenschutz in modernen Zeiten steht. Die Fortschritte der IT-Technologie haben dazu geführt, dass den fast grenzenlosen Möglichkeiten der Kommunikation ein ebenso fast grenzenloses Überwachungsinstrumentarium gegenüber steht. Dieses spannungsgeladene Verhältnis beschränkt sich dabei nicht allein auf die Beziehungen zwischen den staatlichen Behörden einerseits und den Grundrechtsträgern andererseits, sondern zeigt sich ebenso im wirtschaftlichen Alltag zwischen Arbeitgebern und Arbeitnehmern. Man denke an die öffentlichkeitswirksamen Fälle in der jüngeren Vergangenheit: Überwachung des E-Mail-Verkehrs bei der Deutschen Bahn (Logfile-Filterung), Videoüberwachung der Arbeitnehmer beim Lebensmitteldiscounter Lidl durch externe Sicherheitsunternehmen oder Datenscreening und -abgleich bei der Deutschen Telekom (Telekommunikationsverbindungen, Bankdaten und Bewegungsprofile von Aufsichtsräten, Mitarbeitern und Journalisten).

Aus sanktionsrechtlicher Sicht werden Verstöße gegen das Datenschutzrecht häufig mit Geldbußen belegt, also einem Mittel des Ordnungswidrigkeitenrechts. Millionenschwere Zahlungen wie bei Lidl oder der Deutschen Bahn bilden dabei in der Praxis eher die Ausnahme. Noch seltener begegnet man Kriminalstrafen wie im Fall der Deutschen Telekom, wo der verantwortliche Leiter der Konzernsicherheit gemäß § 206 StGB zu einer mehrjährigen Haftstrafe verurteilt wurde.[1] Dieser Tendenz entspricht es auch, dass sich die strafrechtswissenschaftliche Literatur bisher auf datenschutzrechtliche Tatbestände aus dem Bereich der Ordnungswidrigkeiten (§§ 43 BDSG[2], 149 TKG, 16 TMG) konzentriert hat, während Vorschriften des Strafgesetzbuches eher peripher behandelt wurden. Diese Lücke wird durch die verdienstvolle Untersuchung von *Eisele* über die „strafrechtlichen Grenzen der Arbeitnehmerüberwachung" geschlossen.

Ausgehend von der Prämisse, dass „Überwachungsmaßnahmen nicht nur in Rechte von Arbeitnehmern greifen, sondern zugleich auch schutzwürdigen Interessen des Arbeitgebers dienen können", betont der *Autor* am Anfang die Bedeutung der betreffenden Strafvorschriften für die „Compliance", die er – im Einklang mit dem Gesetzgeber[3] – als „Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes" versteht (S. 13). Im Einzelnen untersucht *Eisele* anhand der jeweils einschlägigen Regelungen der §§ 201 ff. StGB die praxisrelevanten Aspekte der Überwachung des Telefon-, des Brief- und des E-Mail-Verkehrs, der Ausforschung gespeicherter Daten sowie der Bildaufnahmen. Dabei geht er nach klassischem Muster vor, indem er einzelne Tatbestandsmerkale sowie Fragen der Rechtswidrigkeit nacheinander darlegt und unter gründlicher Auswertung der Literatur und Rechtsprechung auch eigene Ansätze entwickelt. Im Rahmen des § 201 StGB (Verletzung der Vertraulichkeit des Wortes) vertritt er beispielsweise entgegen der herrschenden Ansicht die Auffassung, dass das Mithören von Telefongesprächen durch Zweithörer, Lautsprecher etc. nicht per se außerhalb des Schutzbereichs der Norm liege, sondern nur dann von einem Tatbestandsausschluss ausgegangen werden könne, „wenn das gesprochene Wort zur Kenntnis des Abhörenden bestimmt ist, was regelmäßig nicht die bloße Kenntnis vom Mithören, sondern ein Einverständnis des Beschäftigten im Sinne einer Zustimmung voraussetzt" (S. 21). Dies gelte unabhängig davon, ob es sich um ein Dienst- oder Privatgespräch handele und ob Letzteres überhaupt erlaubt sei.

In der Frage der Überwachung des E-Mail-Verkehrs und der Ausforschung anderer Computer- und Internetdaten weist *Eisele* auf die umfänglichen Kontrollmöglichkeiten des Arbeitsgebers auf diesem Gebiet hin (S. 26 f.) und arbeitet zunächst den Begriff der Telekommunikation – auch in Abgrenzung zu Telemediendiensten – heraus. Anschließend widmet er sich einer der Hauptproblematiken der Verletzung des Fernmeldegeheimnisses, nämlich dem Unternehmensbegriff bei § 206 StGB: Ist ein Unternehmen, das keine typischen Telekommunikationsdienste anbietet, gleichwohl Adressat der Norm, wenn es über ein internes Telekommunikationssystem verfügt und dieses für seine Mitarbeiter auch zur privaten Nutzung zur Verfügung stellt? Hier positioniert sich der *Autor* ebenfalls gegen die herrschende Meinung und verneint die Anwendbarkeit des § 206 StGB auf Sachverhalte der Privatnutzung durch Arbeitnehmer (S. 31 f.). Auch wenn dadurch angesichts des § 303a StGB („Unterdrücken") keine gravierende Strafbarkeitslücke entsteht, dürfte der entgegengesetzten Ansicht zu folgen sein, da die zulässige private Kommunikation des Arbeitnehmers, die über den Arbeitsplatz erfolgt, grundsätzlich nicht minder schutzbedürftig ist, wie *Eisele* selbst einräumt. Schließlich werden mögliche Rechtfertigungsgründe nach §§ 88 Abs. 3, 91 ff. TKG, 11 ff. TMG sowie nach den allgemeinen Grundsätzen der (mutmaßlichen) Einwilligung umfassend gewürdigt (S. 44 ff.); spätestens in diesem Kontext wird deutlich, dass das Verhältnis zwischen dem Datenschutz- und Telekommunikationsrecht einerseits und dem Strafrecht andererseits noch wenig geklärt und eine aufeinander bezogene Beschäftigung mit beiden Komplexen unumgänglich ist.

Beim Ausspähen von Daten nach § 202a StGB setzt sich *Eisele* ausführlich mit der Verfügungsbefugnis über Daten und der Zugangsverschaffung unter Überwindung der besonderen Sicherung (z.B. Passwort) auseinander (S. 52 ff.). Unter Compliance-Aspekten ist hier von besonderer Bedeutung, dass sich der Arbeitgeber im Bereich der dienstlichen

[1] LG Bonn, Urt. v. 30.11.2010 – 23 KLs 10/10.

[2] Eine Ordnungswidrigkeit nach § 43 BDSG kann zu einer Straftat nach § 44 BDSG hochgestuft werden, wenn der Täter eine in § 43 Abs. 2 BDSG bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, dazu S. 102 ff.

[3] BT-Drs. 17/4230, S. 18.

Kommunikation den Zugriff auf die Passwörter vorbehalten sollte, um sich keinem strafrechtlichen Risiko auszusetzen (S. 55). Ähnliche Probleme kommen auch bei § 303a StGB (Datenveränderung) vor; diesbezüglich schildert der *Autor*, unter welchen Umständen eine Verfügungsbefugnis des Arbeitgebers bei Datenspeicherungen und E-Mails angenommen werden kann (S. 64 ff.). Im Rahmen der Videoüberwachung von Arbeitnehmern gewinnt aus strafrechtlicher Sicht die Regelung des § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) an Bedeutung; doch ebenfalls von Relevanz ist die datenschutzrechtliche Norm des § 6b BDSG (Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen), deren Nicht-Beachtung eine Ordnungswidrigkeit nach § 43 BDSG begründet (S. 72 ff.).

Nach der Darstellung der jeweiligen Straftatbestände widmet *Eisele* den Einzelfragen der Rechtfertigung ein gesondertes Kapitel (S. 76 ff.). Angesichts des wenig geklärten Verhältnisses zwischen dem Datenschutzrecht und dem Strafrecht ist dieser Teil der Untersuchung ein äußerst verdienstvoller. Zu Beginn spricht sich der *Autor* grundsätzlich gegen die Anwendbarkeit der §§ 32, 34 StGB aus, wenn das BDSG hinsichtlich des konkreten Falles eine abschließende, vorrangige Regelung getroffen haben sollte, da diese nicht unterlaufen werden dürfe (S. 76). Anschließend setzt er sich mit den Vorschriften des BDSG auseinander und diskutiert, inwieweit diese als Rechtfertigungsgründe innerhalb des StGB herangezogen werden können. In diesem Kontext kommt der 2009 geschaffenen Regelung des § 32 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) eine hervorgehobene Bedeutung zu (S. 78 ff.). Besonders instruktiv sind *Eiseles* ausführliche Stellungnahmen zu gesetzgeberischen Vorschlägen zur Neuregelung des Beschäftigtendatenschutzes[4] (S. 81 ff.). Es bleibt abzuwarten, ob und in welcher Form der durch Ablauf der Legislaturperiode gegenstandslos gewordene Entwurf in der 18. Legislaturperiode wieder eingebracht wird.[5] Schlussendlich beschäftigt sich der *Autor* mit den einzelnen Anforderungen an eine wirksame Einwilligung des Arbeitnehmers in die Überwachungsmaßnahmen des Arbeitgebers (S. 89 ff.).

Die Untersuchung schließt mit der Analyse der gewonnenen Einzelergebnisse und den daraus zu entnehmenden Folgerungen (S. 96 ff.). Es bedarf keiner hellseherischen Fähigkeiten, um nicht zuletzt in verunsicherten Zeiten der „NSA-Affäre" vorherzusagen, dass die Bedeutung sanktionsrechtlicher und in diesem Zusammenhang auch strafrechtlicher Dimensionen des Datenschutzes stark steigen wird. *Eisele* hat mit seinem Werk eine Grundlagenarbeit vorgelegt, die einen vogelperspektivischen Blick auf die strafbare Arbeitnehmerüberwachung ermöglicht und sicherlich als Ausgangspunkt weiterer Abhandlungen dienen wird.

Privatdozent Jun.-Prof. Dr. Osman Isfen, Bochum

[4] BT-Drs. 17/4230.

[5] Im Koalitionsvertrag kommt jedenfalls ein diesbezüglicher Wille explizit zum Ausdruck: „Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau – auch bei der grenzüberschreitenden Datenverarbeitung – zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen" (Nr. 2.2 „Gute Arbeit – Modernes Arbeitsrecht" unter „Beschäftigtendatenschutz gesetzlich regeln"). Die Bemühungen um den Erlass der dort erwähnten Europäischen Datenschutzgrundverordnung waren übrigens bisher erfolglos; jüngst hat der Rat der Europäischen Union auf seiner Tagung am 10.10.2014 eine partielle allgemeine Ausrichtung zur Datenschutzgrundversorgung angenommen.