Arbeitnehmerdaten im Kernstrafrecht

Zugleich Buchbesprechung zu: *Eisele*, Compliance und Datenschutzstrafrecht*

Franziska Riemer

Trifft schon Arbeitsplatzbewerber das Risiko, von ihrem potentiellen Arbeitgeber unter Zuhilfenahme sozialer Netzwerke genauer unter die Lupe genommen zu werden (dazu *Aumann*, in diesem Heft), so stellt sich das Problem des „Ausgeforscht- und Überwachtwerdens" durch den Arbeitgeber umso intensiver mit Eingehen des Arbeitsverhältnisses.

Strafrechtlich können in diesem Zusammenhang die nebenstrafrechtlichen Bestimmungen des Bundesdatenschutzgesetzes (folgend BDSG) relevant werden. Mit den §§ 43 und 44 verfügt das BDSG sowohl über eine Bußgeld- als auch eine Strafvorschrift. Beide sind insoweit verbunden, als in § 44 BDSG bestimmte Handlungen, welche unter § 43 Abs. 2 BDSG fallen, unter Strafe gestellt werden, sofern der Täter vorsätzlich handelt und die Tat entweder gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht begeht. Zwischen § 44 Abs. 2 BDSG und bereichsspezifischen Straftatbeständen aus dem StGB kann grundsätzlich Tateinheit gem. § 52 StGB bestehen, wobei im Einzelnen umstritten ist, welchen Tatbeständen des StGB gegenüber Subsidiarität besteht.[1] In der Rechtsprechung wurde § 44 Abs. 2 BDSG in Bezug auf den Schutz des Arbeitnehmers am Arbeitsplatz bisher aber kaum relevant.

Im Zusammenhang mit dem Schutz des Arbeitnehmers vor Ausforschungs- und Überwachungsmaßnahmen am Arbeitsplatz ist es daher umso interessanter, auch das Kernstrafrecht in den Blick zu nehmen. Denn auch das Strafgesetzbuch (folgend StGB) enthält mit seinen §§ 201 ff. Normen, die hier Relevanz erlangen können. Der Arbeitgeber kann mit ihnen vor allem dann in Konflikt geraten, wenn die Rechte der Arbeitnehmer und deren Schutzwürdigkeit als Grenze bestimmter innerbetrieblicher Überwachungsmaßnahmen überschritten werden.

Aber wo genau liegen die Grenzen für den Arbeitgeber in Bezug auf die Überwachung des Telefon-, Brief- und E-Mail-Verkehrs seiner Arbeitnehmer? Wie verhält es sich mit Bildaufnahmen oder dem Ausforschen gespeicherter Daten? Und wie verhalten sich Datenschutzrecht und Strafrecht zueinander? Welche Tatbestände können rechtfertigend eingreifen?

Diese Fragen greift nun *Jörg Eisele* in der – soweit ersichtlich – ersten umfassenden Abhandlung zur strafrechtlichen Problematik der Arbeitnehmerüberwachung auf.

Besonders in den Fokus rückt *Eisele* dabei die Frage, ob der Unternehmer als Anbieter von Telekommunikationsdiensten anzusehen ist, wenn er den Arbeitnehmern die Nutzung von Kommunikationsmitteln auch für private Zwecke (wenn auch mit zeitlichen und inhaltlichen Grenzen) gestattet (S. 27 ff.). Da das Strafrecht keinen einheitlichen Unternehmensbegriff kennt und der Begriff vielmehr in den einzelnen Tatbeständen, in denen er genannt wird, nach seinem Kontext zu bestimmen ist, wird hier vorgeschlagen, dass sich der Unternehmerbegriff in § 206 StGB an dem des Telekommunikationsgesetzes (folgend TKG) orientieren soll. Von der Beantwortung dieser Frage – ob ein Unternehmen im Sinne des TKG vorliegt – hängt damit die Anwendbarkeit des § 206 StGB ab.

Eisele zeigt die verschiedenen Meinungen auf (S. 31 ff.) und steht letztlich der Anwendbarkeit eher skeptisch gegenüber. Wenn ein Arbeitgeber seinen Arbeitnehmern auch die private Kommunikation am Arbeitsplatz gestattet, sei einer Meinung nach das TKG gerade nicht anwendbar, da es darin auch um Wettbewerbsaspekte gehe (vgl. § 1 TKG) und entsprechende Dienste i.d.R. entgeltlich erbracht werden (vgl. § 3 Nr. 24 TKG). Auch das Argument der klaren Trennbarkeit zwischen privater und beruflicher Nutzung und damit der Anwendbarkeit verschiedener Gesetze (TKG nur für private, BDSG nur für die berufliche Nutzung) ist nach dieser Ansicht abzulehnen, da sie bei Nutzung desselben Gerätes nicht möglich ist. Letztendlich könnte dies sogar dazu führen, dass eine Kontrolle seitens des Arbeitgebers sich immer am TKG messen lassen müsste, sobald private und berufliche Kommunikation mit demselben Gerät gestattet werden.

Die Vertreter der wohl überwiegenden Ansicht möchten aber, da es auf eine Gewinnerzielungsabsicht bei Erbringung des Telekommunikationsdienstes nicht ankomme und daher auch die unentgeltliche Bereitstellung erfasst sei (vgl. § 3 Nr. 10 TKG), das TKG heranziehen.[2] Der Gesetzesentwurf

* *Eisele,* Compliance und Datenschutzstrafrecht, Strafrechtliche Grenzen der Arbeitnehmerüberwachung (Nomos Schriften zu Compliance Band 3), Baden-Baden 2012.

1 Vgl. *Gola/Schomerus*, Bundesdatenschutzgesetz, 10. Auflage, 2010, § 44, Rn. 2; *Ambs*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze 188. Ergänzungslieferung 2012, § 44, Rn. 4.

2 Dahingehend siehe u.a. *Fischer,* Strafgesetzbuch, 59. Auflage 2012, § 260, Rn. 2.

der Bundesregierung[3] sieht dagegen vor, bei gestatteter Privatnutzung nur das TKG zur Anwendung zu bringen.

Eisele selbst hat trotz seiner erkennbaren Meinung die ausstehenden Neuerungen im Blick und folgt in der weiteren Darstellung der h.M., da es ihm darum geht, die Grenzen für Compliance-Maßnahmen nach geltendem und kommendem Recht darzustellen. Der Gegenansicht muss aber zugestanden werden, dass das Argument der Undurchführbarkeit einer scharfen Trennung zwischen privater und beruflicher Nutzung sehr überzeugend ist. Geht man also von der Anwendbarkeit des § 206 StGB aus, entstehen im Rahmen der Rechtfertigung neue Fragen. Für §§ 206 Abs. 1 und 206 Abs. 2 Nr. 2 StGB könnten Rechtfertigungen im Lichte des § 88 Abs. 3 TKG zu prüfen sein. Folgt man dem, sind dann vor allem die §§ 91 ff. TKG und die §§ 11 ff. Telemediengesetz (TMG), welche jeweils den Schutz personenbezogener Daten regeln, für die Rechtfertigung relevant und das BDSG findet grundsätzlich keine Anwendung.

Nach der Darstellung der relevanten Straftatbestände des StGB (i.V.m. Nebengesetzen) zu den oben aufgeworfenen Fragen geht *Eisele* auch einigen Einzelfragen der Rechtfertigung nach (S. 76 ff.). Es geht hier insbesondere um die Anwendbarkeit der §§ 32, 34 StGB im Rahmen des BDSG, sowie die Regelungen des BDSG und deren Geltung als Rechtfertigungsgründe innerhalb des StGB. In diesem Zusammenhang werden auch Vorschläge zur geplanten Neuregelung des Beschäftigtendatenschutzes (folgend BDSG-E) aufgegriffen und genauer betrachtet.

Die spezifischen Neuregelungen des Beschäftigtendatenschutzes sollen ebenfalls, wie schon § 32 BDSG, für die nicht automatisierte Datenerhebung, -verarbeitung und -nutzung gelten. *Eisele* weist jedoch gleich zu Beginn dieses Abschnitts auf eine weiterhin, auch trotz Erlass eines neuen BDSG, bestehende Schwäche hin (S. 82): Am Verhältnis zum TKG soll sich nichts ändern, was bedeutet, dass das BDSG(-E) ohnehin nur dann Anwendung findet, wenn eine Privatnutzung (siehe dazu das Beispiel oben) nicht gestattet ist. Zu Recht schreibt er, dass eine Differenzierung nach privater und dienstlicher Nutzung nicht überzeugen kann, gerade weil auch der Gesetzgeber im BDSG-E nun einige Details regeln möchte. Sie liefen ins Leere, wäre das Gesetz nicht anwendbar. Es entstünde nämlich eine Lage, in der detaillierte Regelungen (BDSG-E) einem spezielleren Gesetz (TKG) gegenüberstünden. Nach dem Grundsatz des Vorrangs des spezielleren Gesetzes wären die detailreicheren Regelungen dann nicht anwendbar. Zur Lösung dieser wohl kaum gewollten Lage wären zwei Möglichkeiten denkbar: Entweder eine Änderung im TKG bezüglich der Vorrangregelung gegenüber dem BDSG-E oder eine explizite Erwähnung eines Vorrangs aufgrund von Spezialität im BDSG-E.

Mit Blick auf die Heranziehung von BDSG(-E)-Normen für die Rechtfertigung im Rahmen von StGB-Tatbeständen (S. 77ff.) ist es aufgrund des Prinzips der Einheit der Rechtsordnung grundsätzlich erforderlich, dass eine datenschutzrechtlich erlaubte Maßnahme nicht dazu führen kann, dass mit ihrer Durchführung zugleich eine Straftat begangen wird. Pauschal lassen sich die durch das BDSG(-E) erlaubten Handlungen jedoch nicht zur Rechtfertigung der Verwirklichung von Straftatbeständen heranziehen. Es kommt vielmehr darauf an, ob auf strafrechtlicher Ebene noch weitere Merkmale hinzutreten. Beispielhaft ist hier der Fall, dass der Arbeitgeber, der die Telekommunikation ausschließlich zu beruflichen Zwecken erlaubt hat, stichprobenartig Daten erhebt, weil er dies zur Leistungs- und Verhaltenskontrolle eines bestimmten Arbeitnehmers für erforderlich hält und keine Anhaltspunkte bestehen, dass ein schutzwürdiges Interesse dieses Arbeitnehmers das ausschließt.
§ 32i Abs. 3 BDSG-E ermöglicht eine solche Maßnahme. Überwindet der Arbeitgeber hierzu jedoch eine Zugangssicherung i.S.d. § 201 a StGB (z.B. das persönliche Passwort des Arbeitnehmers), kann aus der datenschutzrechtlichen Erlaubnis keine Rechtfertigung für die Straftat gezogen werden.

Eine Einwilligung (S. 89 ff.) in Maßnahmen nach BDSG wirkt auch mit Blick auf Straftatbestände des StGB tatbestandsausschließend oder rechtfertigend.[4] Insbesondere haben auch die geplanten Neuerungen im BDSG – konkret geht es hier um geplante Einschränkungen bei der Einwilligung – auf das Kernstrafrecht keine Auswirkungen, denn das kernstrafrechtlich betroffene Rechtsgut bleibt ungeachtet eines Datenschutzverstoßes disponibel. Die Strafbarkeit nach BDSG würde jedoch mit den diskutierten Neuerungen in weiteren Fällen zum Tragen kommen, da es insofern gerade um BDSG-spezifische Schutzgüter geht.

Zum Schluss geht *Eisele* noch auf die europäische Perspektive und dortige Tendenzen ein (S. 105 f.). Zwar finden sich im materiellen Strafrecht Angleichungen, so dass Unternehmen, die über die Grenzen eines Landes hinaus agieren, stets ähnlichen Regelungen ausgesetzt sind. Die europäische Datenschutzrichtlinie (95/46 EG) enthält aber keine spezifischen Regelungen zum Beschäftigtendatenschutz und keine detaillierten Sanktionsvorgaben.

An diesem Punkt wurde *Eisele* jedoch teilweise von der allgemeinen Rechtsentwicklung überholt: Nicht nur auf nationaler, sondern auch auf Ebene der europäischen Union wird derzeit an Neuerungen gearbeitet. Es ist wohl dem Redaktionsschluss (Dezember 2011) geschuldet, dass sich in seinem Buch keine Hinweise auf den am 25.1.2012 von der EU-Kommission veröffentlichten Vorschlag zu einer Datenschutzgrundverordnung (DS-GVO), welche an die Stelle der Datenschutzrichtlinie treten soll, finden.

Inwiefern die Änderungen, welche die DS-GVO in das deutsche Recht einbringen wird (dazu auch *Splinter*, in diesem Heft), sich auf das dargestellte Kernstrafrecht auswir-

3 BT-Drs. 17/4230, S. 42 f.

4 Allgemeines zur Einwilligung im StGB z.B. bei *Rengier,* Strafrecht AT, 3. Auflage 2011, § 23.

ken könnten, bleibt bei *Eisele* damit offen.

Im strafrechtlichen Kontext liegen diese Berührungspunkte zwischen Kernstrafrecht und Datenschutzrecht wie gesehen v.a. bei der Auslegung einzelner Tatbestandsmerkmale (u.a. § 206 StGB), sowie auf der Ebene der Rechtfertigung. Ändert sich das Datenschutzrecht nun durch Unionsrecht, so bleibt abzuwarten, welche Rückwirkungen dies angesichts der Berührungspunkte auf die nationale Strafrechtsordnung haben wird. Zumindest für die Ebene der Rechtfertigung kann aber wohl hier schon festgehalten werden, dass der Einfluss des europäischen Rechtsakts begrenzt sein wird, denn an den Kriterien der strafrechtlichen Einwilligung ändert eine europäische Verordnung zum Datenschutz nichts.

Ein „Abschied von den Grundrechten"?

Ausblick auf den Grundrechtsschutz nach der EU-Datenschutzgrundverordnung

Markus Vordermayer

Die geplante EU-Datenschutzgrundverordnung (DS-GVO-E)[1] wird den Datenschutz – und insbesondere die grundrechtliche Komponente desselben – auf eine neue Grundlage stellen. Der Richter am Bundesverfassungsgericht *Johannes Masing* hat in diesem Zusammenhang bereits Anfang des Jahres die Diskussion angestoßen, inwiefern ein solch „technisch" anmutendes Gesetzgebungsprojekt auf kaltem Wege verfassungsrelevante Änderungen in der europäischen Grundrechtsarchitektur vornehmen könnte und gar ein „Abschied von den [deutschen] Grundrechten" droht[2]. Ein solcher würde insbesondere auch den hier im Vordergrund stehenden *Schutz privater Daten im Internet* betreffen. Die ausnehmend kritische Perspektive von Masing soll im Folgenden als Ausgangspunkt dienen, einen Blick auf den materiellen Grundrechtsstandard nach Annahme der zur Diskussion stehenden Verordnung (I.) und die prozessualen Durchsetzungsmöglichkeiten desselben (II.) zu werfen.

I. Anwendbare Grundrechte und materieller Grundrechtsstandard

Wie auch *Masing* unterstellt, ist davon auszugehen, dass mit der Annahme des Kommissionsvorschlags durch Parlament und Rat die Grundrechte des Grundgesetzes (GG) im Anwendungsbereich der Verordnung[3] grds. außer Anwendung geraten.[4] Mit der geplanten Umstellung des europäischen Rechtssatzes von einer Richtlinie[5] auf eine Verordnung, deren weitgefasstem Anwendungsbereich[6] und nur wenigen Abweichungsmöglichkeiten für die Mitgliedstaaten[7] würden die nationalen Grundrechte in einer besonders weit ausgreifenden Materie[8] ihre Maßstabsfunktion verlieren.[9] Zwar ist es unter Hinweis auf die „Schutzniveauklausel" des Art. 53 GRCh heute teilweise umstritten, inwiefern diese eine Renaissance nationaler Grundrechte

1 Allgemein zum Entwurf und den gegenwärtig bestehenden Regelungen siehe *Sommerrock*, in diesem Heft.

2 „Ein Abschied von den Grundrechten", SZ v. 9.1.2012, 10.

3 Zur Bindung an die Unionsgrundrechte nach Art. 51 Abs. 1 S. 1 GRCh („bei der Durchführung des Rechts der Union") vgl. *Jarass*, Grundrechte-Charta, 2010, Art. 51 Rdn. 16 ff.; zur EuGH-Rspr. vor Geltung der GRCh („im Anwendungsbereich des Unionsrechts") vgl. *Calliess*, JZ 2009, 113 (115).

4 Die Frage, ob der Entwurf in seiner ggw. Fassung kompetenzgemäß erlassen werden könnte, soll im Folgenden außer Betracht bleiben; vgl. nur *Franzen*, DuD 2012, 322 (325 f.).

5 Zu den einschlägigen Richtlinien, insbesondere der DS-Richtlinie 95/46/EG siehe *Sommerrock*, in diesem Heft.

6 Art. 2 DSGVO-E.

7 Vgl. *Hornung*, ZD 2012, 99 (100); z.B. Art. 80, 82 DSGVO-E; vgl. auch *Splinter*, in diesem Heft.

8 Zum Datenschutz als Querschnittsmaterie *Spiecker* gen. Döhmann/*Eisenbarth,* JZ 2011, 169; *Britz*, EuGRZ 2009, 1 (4).

9 Vgl. *Hornung* (Fn. 7), 100. Zwar erscheint fraglich, ob sich damit ggü. der vom EuGH mit einem weiten Anwendungsbereich versehenen und als grds. abschließende Harmonisierung verstandenen (ggw. geltenden) DS-Richtlinie substantiell etwas ändert – zumindest hinsichtlich einer möglichen verbleibenden Bindung an nationale Grundrechte im Umsetzungsspielraum der (jetzigen) Richtlinie (so z.B. *Calliess* [Fn. 3], 120) bleibt dies jedoch relevant; vgl. insgesamt dazu *Britz* (Fn. 8), 4 f.; *Siemen*, EuR 2004, 306 (312 f.).