BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 16
April 2012

zu der Vorschrift des § 32 d Abs. 3 BDSG-E des Gesetzentwurfs der Bundesregierung vom 15.12.2010 (BT-Drucksache 17/4230)

Mitglieder des Strafrechtsausschusses

RA Prof. Dr. Dr. Alexander Ignor, Vorsitzender (Berichterstatter)
RA Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm (Berichterstatter)
RA Thomas C. Knierim
RA Dr. Daniel M. Krause
RA Prof. Dr. Holger Matt
RAin Anke Müller-Jacobsen
RA Prof. Dr. Tido Park
RA Prof. Dr. Reinhold Schlothauer
RA Dr. Jens Schmidt
RAin Dr. Anne Wehnert (Berichterstatterin)
RAin Dr. Annette von Stetten
RA Frank Johnigk, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Justiz
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Redaktionen der NJW, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag, Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit zurzeit rund 157.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen - auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

I.

Der Gesetzentwurf der Bundesregierung zur Regelung des Beschäftigtendatenschutzes (BT-Drucksache 17/4230 vom 15.10.2010) sieht Neuregelungen (§§ 32 a bis 32 l BDSG-E) für den Umgang mit Beschäftigtendaten vor, die Eingang in das BDSG finden und die bisherige zentrale Norm des § 32 BDSG ergänzen sollen. Diese Stellungnahme beschränkt sich auf die Vorschrift des § 32 d Abs. 3 BDSG-E.

§ 32 d Abs. 3 BDSG-E sieht folgenden Wortlaut vor:

> *„Der Arbeitgeber darf zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigtenverhältnis, insbesondere zur Aufdeckung von Straftaten nach den §§ 266, 299, 331 bis 334 des Strafgesetzbuches, einen automatisierten Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form mit von ihm geführten Daten durchführen. Ergibt sich ein Verdachtsfall, dürfen die Daten personalisiert werden. Der Arbeitgeber hat die näheren Umstände, die ihn zu einem Abgleich nach Satz 1 veranlassen, zu dokumentieren. Die Beschäftigten sind über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu unterrichten, sobald der Zweck durch die Unterrichtung nicht mehr gefährdet wird.“*

Die Bundesrechtsanwaltskammer lehnt den Gesetzentwurf insoweit ab.

II.

1. Vorbemerkungen

Die Datenschutzskandale, die sich in der jüngsten Vergangenheit in großen deutschen Unternehmen ereignet haben, machen deutlich, welche Brisanz und Aktualität das Thema Beschäftigtendatenschutz in der Praxis hat. Nach der amtlichen Begründung des Gesetzentwurfs sollen die Beschäftigten durch die Neuregelungen vor Bespitzelungen am Arbeitsplatz und der unzulässigen Erhebung und Verwendung ihrer personenbezogenen Daten geschützt werden (BT-Drucksache 17/4230, S. 1). Dieses Ziel wird durch die Vorschrift des § 32 d Abs. 3 BDSG-E nicht erreicht, sondern geradezu in ihr Gegenteil verkehrt. Durch den Wegfall des Erfordernisses eines konkreten Anfangsverdachts sollen nunmehr flächendeckend verdachtslose, automatisierte Datenabgleiche gestattet sein, die praktisch an keine weiteren gesetzlichen Voraussetzungen gebunden sind. Dies stellt für den Arbeitnehmer eine erhebliche Verschlechterung gegenüber der aktuellen Gesetzeslage dar und ist mit verfassungsrechtlichen Grundsätzen nicht zu vereinbaren. Die Vorschrift des § 32 d Abs. 3 BDSG-E soll offenbar genau die Kontroll- und Überwachungsmaßnahmen ermöglichen, die im Rahmen der jüngsten

Datenschutzskandale eine breite Empörung in der Öffentlichkeit hervorgerufen und gerade den Anstoß für eine Reform des Beschäftigtendatenschutzes gegeben haben.

2. Besondere Grundrechtsrelevanz als Ausgangspunkt des Beschäftigtendatenschutzes

Der Beschäftigtendatenschutz betrifft die Erfassung besonders sensibler, persönlicher Daten und ist daher ein Bereich von hoher Grundrechtsrelevanz. Um den Gefahren, die durch elektronische Datenverarbeitungsprozesse für die Freiheitsgrundrechte der Bürger entstehen, in angemessener Weise begegnen zu können, hat das BVerfG aus Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG zwei Grundrechte entwickelt, zum einen das Grundrecht auf informationelle Selbstbestimmung (vgl. nur BVerfGE 65, 1 ff.), zum anderen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. nur BVerfG NJW 2008, 822 ff.).

Das Recht auf informationelle Selbstbestimmung gewährleistet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. In Anbetracht der Möglichkeiten der modernen Datenverarbeitung muss der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe geschützt werden (vgl. BVerfGE 65, 1 ff.).

Dieser Schutz wird durch das vom BVerfG im Jahre 2008 entwickelte sog. „IT-Grundrecht" ergänzt, das den neuen Persönlichkeitsgefährdungen durch die zunehmende Verbreitung vernetzter informationstechnischer Systeme begegnen will. Danach ist insbesondere das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben, geschützt, soweit dies nicht durch andere Grundrechte – insbesondere das Recht auf informationelle Selbstbestimmung – gewährleistet werden kann (vgl. BVerfG NJW 2008, 822, 827). Dieser Schutz bezieht sich auf alle IT-Systeme, die der Bürger entweder in privater oder in betrieblicher Hinsicht nutzt.

Die genannten Grundrechte sind nicht schrankenlos gewährleistet. Der Einzelne hat keine absolute, uneingeschränkte Herrschaft über „seine" Daten, da seine Persönlichkeit innerhalb einer sozialen Gemeinschaft stets ein Abbild der sozialer Realität ist und die in diesem Zusammenhang erlangten personenbezogenen Informationen nicht ausschließlich dem Betroffenen allein zugeordnet werden können (BVerfGE 65, 1 ff.). Beschränkungen bedürfen allerdings einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar ergeben (vgl. BVerfGE 45, 400, 420). Einschränkungen sind nur zulässig im überwiegenden Allgemeininteresse und müssen dem Grundsatz der Verhältnismäßigkeit Rechnung tragen. Daraus folgt, dass jede Datenerhebung nur bis zu dem Maß zulässig ist, das für die Erfüllung einer bestimmten Aufgabe erforderlich ist (Erforderlichkeitsprinzip). Nach dem Gebot der Zweckbindung muss sichergestellt werden, dass die Daten nur zu legitimen und nachvollziehbaren Zwecken erhoben bzw. verwendet werden. Der Kernbereich der privaten Lebensgestaltung muss dabei stets unangetastet bleiben. Alle einfachgesetzlichen Regelungen, die die „Datenschutz-Grundrechte" einschränken, müssen diesen Anforderungen genügen.

Diese Grundsätze gelten nicht nur im Verhältnis Staat-Bürger, sondern im Wege der mittelbaren Drittwirkung auch innerhalb des Beschäftigungsverhältnisses (vgl. BAG NJW 2003, 3436). Um den verfassungsrechtlichen Anforderungen des Grundgesetzes und der Rechtsprechung des BVerfG zu entsprechen, hat das BAG eine Totalüberwachung eines Arbeitnehmers für unzulässig erklärt (vgl. BAG NJW 2008, 2732, 2734). Werden die Grundrechte der Arbeitnehmer auf Datenschutz durch Datenerhebungen des Arbeitgebers eingeschränkt, ist im

Rahmen der Rechtfertigung eines solchen Eingriffs stets eine Abwägung der Interessen von Arbeitgeber und Arbeitnehmer vorzunehmen, in der die datenschutzrechtlichen Belange der Arbeitnehmer in ausreichendem Maße berücksichtigt und in einen angemessenen Ausgleich gebracht werden müssen (BArbG NJW 2003, 3436, 3437). Es ist Aufgabe des Gesetzgebers, die Einhaltung dieser Grundsätze durch gesetzliche Regelungen sicherzustellen.

3. Kritische Stellungnahme

a) Bedenkliche Relativierung des staatlichen Verarbeitungsmonopols zur Aufklärung von Straftaten

Die Aufklärung von Straftaten ist eine staatliche Aufgabe. Sie obliegt den Strafverfolgungsbehörden. Die öffentlich-rechtliche Pflicht zur Verfolgung von Straftaten ist Ausdruck des staatlichen Gewaltmonopols, das auch ein Verarbeitungsmonopol für die Aufklärung von Straftaten beinhaltet (vgl. nur Hassemer NJW 1985, 1921, 1924). Dieses Verarbeitungsmonopol wird ohne die Macht des Staates, die rechtliche Relevanz von Konflikten zu definieren, die Verarbeitung dieser Konflikte an sich zu ziehen und die Formen der Konfliktverarbeitung festzulegen sowie auch private Dritte notfalls fernzuhalten, konterkariert.

In jeder Übertragung von Befugnissen zur Untersuchung und Aufklärung von Straftaten auf nichtstaatliche Stellen liegt eine Relativierung des staatlichen Verarbeitungsmonopols. Denn neben das staatliche Verfahren tritt ein nichtstaatliches, von Privaten ausgestaltetes Verfahren, das nicht dem mit rechtsstaatlichen Schutzmechanismen ausgestatteten Prozessrecht folgt, sondern eigenen, selbstgeschaffenen Regeln. Dies kann nicht nur für die Rechtsposition der Betroffenen einschneidende Auswirkungen haben, sondern auch für die Verwertbarkeit der erlangten Beweise.

Im Gesetzentwurf zu § 32 d Abs. 3 BDSG-E heißt es, der Arbeitgeber „darf“ einen Abgleich von Daten durchführen. Diese Formulierung suggeriert, dass die Anordnung eines Datenscreenings im Ermessen des Arbeitgebers steht. Tatsächlich aber dürfte das durch den Entwurf suggerierte Ermessen über die Vorschrift des § 130 OWiG zu einer Rechtspflicht zur Durchführung derartiger Überwachungsmaßnahmen erstarken. Nach § 130 Abs. 1 OWiG handelt ordnungswidrig, wer als Inhaber eines Betriebes oder Unternehmens Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern. Das Ausmaß der Aufsichts- und Organisationspflichten hängt wesentlich auch von den Überwachungsmöglichkeiten ab. Der Betriebsinhaber ist verpflichtet, die durchführbaren und zumutbaren Organisationsmaßnahmen, die zur Beachtung der Rechtsordnung erforderlich und geeignet sind, zu ergreifen (vgl. nur Göhler, OWiG, § 130 Rn 10 mwN). Je weitergehender die Überwachungsmöglichkeiten in einem Unternehmen sind, umso höher sind die Anforderungen an die bußgeldbewehrten Pflichten nach § 130 OWiG. Vor diesem Hintergrund ist zu besorgen, dass der Betriebsinhaber über die Vorschrift des § 130 Abs. 1 OWiG einer Pflicht zur Durchführung von Datenscreenings gegen seine Mitarbeiter unterliegen kann, was nicht nur zu einer flächendeckenden Überwachung von Mitarbeitern in der Wirtschaft führen würde, sondern auch zu einem fragwürdigen Zwang zur Selbstbelastung von Wirtschaftsunternehmen und deren Führungskräften. Dies wäre nicht nur unter dem Gesichtspunkt des staatlichen Verarbeitungsmonopols problematisch, sondern auch unter dem Aspekt des Nemo-tenetur-Gebots.

b) Keine Mitarbeiterscreenings ohne konkreten Tatverdacht

Nach der geltenden Regelung des § 32 Abs. 1 S. 2 BDSG dürfen personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn „zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen“, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Hierfür genügt der allgemeine Verdacht, dass irgendjemand im Unternehmen einen strafrechtlichen Sachverhalt verwirklicht hat, nicht. Auch rein präventive Datenabgleiche zur Korruptionsbekämpfung oder zur Identifizierung von „Problembereichen“ in Unternehmen ohne tatsächliche Anhaltspunkte für einen begangenen Rechtsverstoß sind derzeit unzulässig, soweit der Datenzugriff personenbezogene oder personenbeziehbare Beschäftigtendaten zum Gegenstand hat.

Die Vorschrift des § 32 d Abs. 3 BDSG-E lässt Mitarbeiterscreenings ohne konkreten Tatverdacht zu und legalisiert damit eine anlasslose und dauerhafte „Rasterfahndung“ in Unternehmen. Ein verdachts- und anlassloses Mitarbeiterscreening ist indes verfassungsrechtlich problematisch. Der automatisierte Abgleich von Beschäftigtendaten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers dar, der nach allgemeinen verfassungsrechtlichen Grundsätzen einer Rechtfertigung bedarf. Dies bedeutet, dass Screenings der beabsichtigten Art nur aufgrund einer gesetzlichen Grundlage und zu einem im überwiegenden allgemeinen Interesse liegenden Zweck vorgenommen werden dürfen. Dabei muss der Grundsatz der Verhältnismäßigkeit gewahrt werden und eine Abwägung der berechtigten Interessen von Arbeitgeber und Arbeitnehmer erfolgen. Diesen verfassungsrechtlichen Anforderungen wird die Vorschrift des § 32 d Abs. 3 BDSG-E nicht gerecht.

Nach geltender Gesetzeslage in § 32 Abs. 1 S. 2 BDSG wird der Eingriff durch einen konkreten Straftatverdacht gerechtfertigt. Damit wird sichergestellt, dass Datenscreenings von einem im Allgemeininteresse liegenden Zweck abhängig sind, nämlich zur Aufklärung von Straftaten. Existiert ein konkreter Tatverdacht gegen einen bestimmten Mitarbeiter, so überwiegen die Informations- und Aufklärungsinteressen des Arbeitgebers die Datenschutzrechte des Betroffenen. Da dieser Tatverdacht nach § 32 Abs. 1 S. 2 BDSG „zu dokumentieren“ ist, ist auch die Transparenz und Überprüfbarkeit gewährleistet.

Mit dem Wegfall des Erfordernisses eines konkreten Anfangsverdachts wird die verfassungsrechtliche Balance zwischen den grundrechtlichen Datenschutzrechten des Arbeitnehmers einerseits und den Interessen des Arbeitgebers andererseits aufgegeben. Der Arbeitgeber kann gewissermaßen ins Blaue hinein ohne zeitliche Begrenzung flächendeckend Datenscreenings gegen seine Arbeitnehmer durchführen, ohne dass eine sinnvolle Begrenzung im Interesse des Arbeitnehmerdatenschutzes erkennbar ist. Ein verdachts- und anlassloses Datenscreening begründet die Gefahr einer flächendeckenden Totalüberwachung der Beschäftigten, die im Hinblick auf die grundrechtlich geschützten Datenschutzrechte der Arbeitnehmer jeder Verhältnismäßigkeit entbehrt. Eine flächendeckende und anlasslose „Rasterfahndung“ in Unternehmen führt nur dazu, dass sich die Mitarbeiter einem Generalverdacht ausgesetzt sehen. Ausforschung und Totalüberwachung von Beschäftigten sollten durch den Gesetzentwurf eigentlich verhindert und nicht gefördert werden.

Die verfassungsrechtlichen Bedenken werden auch nicht durch die „Formulierungsvorschläge“ des Bundesministeriums der Justiz vom 07.09.2011 beseitigt. Denn auch in diesen „Formulierungsvorschlägen“ wird nicht an einen konkreten Anfangsverdacht angeknüpft, sondern das Datenscreening von einer „aufgrund einer zu dokumentierenden Risikoanalyse erkannten konkreten Gefahr der Begehung von Straftaten nach den §§ 266, 299, 331 bis 334 des StGB oder anderen schwerwiegenden Pflichtverletzungen“ abhängig gemacht. Mit dem Erfordernis einer in einer „Risikoanalyse erkannten konkreten Gefahr“ wird das Kind gewissermaßen mit dem Bade ausgeschüttet. Während der Gesetzentwurf der Bundesregierung vom 15.10.2010 (BT-Drucks. 17/4230) ein Datenscreening ausschließlich zur (repressiven) „Aufdeckung von Straftaten“ vorsieht, soll nun durch bloße „Formulierungsvorschläge“ auch ein Datenscreening zur präventiven Verhinderung von Rechtsverletzungen eingeführt werden. Hierdurch wird die klare Trennung zwischen der Aufklärung bereits begangener Rechtsverstöße einerseits und der Verhinderung zukünftiger Rechtsverstöße andererseits in bedenklicher Weise aufgegeben. Der Umstand, dass mit ergänzenden „Formulierungsvorschlägen“ ein tief in grundrechtliche Gewährleistungen eingreifendes Überwachungsinstrument – entgegen der Konzeption des ursprünglichen Gesetzentwurfs – von einem Mittel zur Aufklärung von Straftaten in ein Präventionsinstrumentarium umgewandelt wird, zeigt, wie wenig durchdacht das Gesamtkonzept des Gesetzesvorhabens ist.

c) Anonymität bzw. Pseudonymität nicht sichergestellt

Auch die Regelungen, wonach die erhobenen Daten zunächst anonymisiert bzw. pseudonymisiert erhoben und erst bei einem konkreten Verdacht personalisiert werden sollen, bieten für die Betroffenen keinen ausreichenden Schutz. Denn der Gesetzentwurf enthält keine Vorgaben für ein praktikables und nachvollziehbares Verfahren, mit dem die vollständige Anonymität bzw. Pseudonymität sichergestellt werden kann. Damit drohen erhebliche Missbrauchsgefahren, insbesondere die Gefahr der Ausforschung von Mitarbeitern. Gerade bei kleinen Unternehmen mit einer geringen Mitarbeiterzahl ist es naheliegend, dass im Rahmen der Auswertung der Daten Rückschlüsse auf bestimmte Mitarbeiter möglich sind. Aber auch bei größeren Unternehmen ist die umfassende Anonymität der Mitarbeiter im Rahmen des Datenabgleichs – wie es der Wortlaut des § 32 d Abs. 3 S. 1 BDSG-E suggeriert – keineswegs gewährleistet. Insbesondere ist der Rückgriff auf die in den Vorschriften der § 3 Abs. 6 BDSG und § 3 Abs. 6 a BDSG enthaltenen Legaldifinitionen für die Begriffe des „Anonymisierens“ und „Pseudonymisierens“ problematisch. Nach § 3 Abs. 6 BDSG ist unter „Anonymisieren“ das Verändern personenbezogener Daten derart zu verstehen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. „Pseudonymisieren“ ist nach § 3 Abs. 6 a BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Beide Definitionen setzen begriffsnotwendig voraus, dass der Personenbezug entweder überhaupt nicht oder nur mit unverhältnismäßig großem Aufwand hergestellt werden kann. Um jedoch eine praktikable und schnelle Repersonalisierung im Verdachtsfall nach § 32 d Abs. 3 S. 2 BDSG-E zu ermöglichen, muss der Rückbezug auf einen bestimmten Mitarbeiter ohne großen Aufwand durchführbar sein, anderenfalls könnte der Gesetzentwurf sein Ziel nicht erreichen. Da die Anonymität der Daten aber eine rasche Rekonstruktion des Personenbezugs ausschließt, kann eine solche schon per definitionem nicht vorliegen. Durch die Verwendung der beiden Begriffe in § 32 d Abs. 3 S. 1 BDSG-E wird dem Betroffenen ein wirksamer Schutz vor Ausforschung suggeriert, der im Hinblick auf die Möglichkeiten und Erfordernisse der Repersonalisierung in § 32 d Abs. 3 S. 2 BDSG-E aber nicht in dieser weitreichenden Form beabsichtigt sein kann.

Besonders bedenklich sind die Formulierungsvorschläge des Bundesministeriums der Justiz vom 07.09.2011, in denen der anonymisierte Abgleich mit der Parenthese „– soweit möglich –“ versehen wird, also unter den Vorbehalt der „Möglichkeit“ gestellt wird. Ob der Abgleich in anonymisierter Form „möglich“ ist oder nicht, obliegt der alleinigen Entscheidung des Arbeitgebers. Damit aber ist der Arbeitnehmer dem personalisierten Datenzugriff durch seinen Arbeitgeber schutzlos ausgeliefert. Ein flächendeckendes, verdachtsunabhängiges Datenscreening gegen Mitarbeiter eines Unternehmens ohne zwingende Gewährleistung der Anonymität des Datenabgleichs ist evident verfassungswidrig.

d) Keine Verhältnismäßigkeitsprüfung vorgesehen

Weiterhin ist zu beanstanden, dass in § 32 d Abs. 3 BDSG-E keine Verhältnismäßigkeitsprüfung vorgesehen ist. Damit genügt die Vorschrift nicht den Anforderungen des BVerfG und BAG, wonach die Erhebung, Verarbeitung und Verwendung von Daten nur dann rechtmäßig ist, wenn sie für die Erfüllung der Aufgaben des Verwenders bzw. des Arbeitgebers erforderlich ist und zum verfolgten legitimen Zweck in einem angemessenen Verhältnis steht (vgl. BVerfG NJW 1983, 1307; BAG NJW 2003, 3436, 3437).

Um den Vorgaben zu genügen, ist eine Gewichtung der zulässigen Maßnahmen z.B. nach der Schwere der Straftat, der Schwere des Tatverdachts oder der Anzahl der betroffenen Mitarbeiter (Streubreite der Maßnahme) unerlässlich. Da in der Praxis genau an diesem Punkt Unsicherheiten hinsichtlich der Art und des zulässigen Umfangs von Datenabgleichen auftreten, wäre es erforderlich gewesen, dass der Gesetzgeber die Norm insoweit konkreter gefasst hätte. Die Vorschrift des § 32 Abs. 1 S. 2 BDSG sieht in der geltenden Gesetzesfassung ausdrücklich eine Interessenabwägung zwischen dem Interesse des Arbeitgebers an der Aufklärung und den Interessen des Betroffenen vor. Wenn in der Vorschrift des § 32 d Abs. 3 BDSG-E auf eine Interessenabwägung bzw. auf eine Verhältnismäßigkeitsprüfung vollständig verzichtet wird, werden die Interessen des Arbeitgebers an Überwachung und Bespitzelung der Beschäftigten in den Vordergrund gestellt, während die Datenschutzbelange der Mitarbeiter in unzulässiger Weise zurücktreten müssen. Auch wenn man legitime Informationsinteressen des Arbeitgebers prinzipiell anerkennen mag, so darf die Abwägung nicht einseitig zu Lasten der Persönlichkeitsrechte der Arbeitnehmer erfolgen.

e) Merkmal der „schwerwiegenden Pflichtverletzung“ zu unbestimmt

Die Regelung in § 32 d Abs. 3 S. 1 BDSG-E, wonach der Arbeitgeber flächendeckende Datenscreenings auch zur Aufdeckung „anderer schwerwiegender Pflichtverletzungen“ durchführen darf, begegnet erheblichen Bedenken. Der unbestimmte Rechtsbegriff der „anderen schwerwiegenden Pflichtverletzungen“ führt in der Praxis zu Auslegungsschwierigkeiten und damit zu Rechtsunsicherheit. Hinzukommt, dass bloße zivilrechtliche Vertragsverletzungen ohne strafrechtliche Relevanz einen solch tiefgreifenden Eingriff in die Persönlichkeitsrechte des Arbeitnehmers unter keinen Umständen rechtfertigen können.

Nach der Begründung des Gesetzentwurfs kann unter den Begriff der „Pflichtverletzung“ auch eine Ordnungswidrigkeit fallen, wenn diese von einiger Erheblichkeit ist. Unter welchen Voraussetzungen und bei welchen Ordnungswidrigkeitentatbeständen die Erheblichkeitsschwelle überschritten ist, bleibt jedoch offen. Das Ziel des Gesetzgebers, durch klare Regelungen die Rechtssicherheit zu erhöhen, kann mit solchen Blanketten keinesfalls erreicht werden. Angesichts der hohen Grundrechtsrelevanz des automatisierten Datenabgleichs und der sich aufdrängenden Missbrauchsgefahren ist die präzise Normierung der Eingriffsvoraussetzungen unverzichtbar. Auch wenn in der Gesetzesbegründung ausgeführt wird, dass die gewählte Formulierung an die Vorschrift des § 626 BGB habe anknüpfen wollen, so führt dies nicht weiter. Die arbeitsgerichtliche Rechtsprechung stellt an das Merkmal des „wichtigen Grundes“ keine hohen Anforderungen (vgl. nur BAG NZA 2010, 1227 „Fall Emmely“), so dass bereits bei Bagatellverstößen ein Datenscreening gerechtfertigt wäre. Dass dies unter Verhältnismäßigkeitsgesichtspunkten nicht zulässig sein kann, liegt auf der Hand.

f) § 32 d Abs. 3 S. 4 BDSG als Verstoß gegen das sog. Transparenzgebot

Nach der Vorschrift des § 32 d Abs. 3 S. 4 BDSG-E sind die Arbeitnehmer über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu unterrichten, sobald der Zweck durch die Unterrichtung nicht mehr gefährdet wird. Durch diese Formulierung wird dem Transparenzgebot nicht in ausreichendem Maße Rechnung getragen, da der Arbeitgeber unter Hinweis auf eine angebliche Gefährdung des möglicherweise erst in ferner Zukunft erreichbaren Zwecks eine Benachrichtigung der Beschäftigten immer wieder aufschieben könnte. Dem sog. Transparenzgebot kann nur dann Rechnung getragen werden, wenn die Mitteilungspflichten nicht vom Erreichen eines vom Arbeitgeber selbst definierten Untersuchungszwecks, sondern objektiv von der Beendigung der Maßnahme und/oder Repersonalisierung der verwendeten Daten abhängig gemacht wird.

g) Keine nachvollziehbare Auflösung des Spannungsverhältnisses zwischen Compliance einerseits und Datenschutz andererseits

Der Begründung des Gesetzentwurfs lässt sich entnehmen, dass die Vorschrift des § 32 d Abs. 3 BDSG-E eine Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen darstellen soll (BT-Drucksache 17/4230, S. 18). Dennoch ist es der Bundesregierung im Hinblick auf die oben angesprochenen Defizite des Entwurfs nicht gelungen, den Beschäftigtendatenschutz in diesem Sinne weiterzuentwickeln und einen angemessenen Ausgleich zwischen den Erfordernissen einer effektiven Compliance und dem Datenschutz zu erreichen. Dem Entwurf gelingt es nicht, das zwischen beiden Gebieten bestehende Spannungsverhältnis aufzulösen, obwohl es gerade in diesem sensiblen Bereich geboten gewesen wäre, der Praxis präzise Vorgaben an die Hand zu geben.

Auch wenn im Gegensatz zum Referentenentwurf des BMI vom 28.05.2010 ein Datenabgleich zur *Verhinderung* von Straftaten oder Pflichtverletzungen nicht mehr vorgesehen ist, legt der sehr weitgehende Wortlaut der aktuellen Entwurfsfassung des § 32 d Abs. 3 BDSG-E nahe, dass auch präventive Maßnahmen umfasst sind. In diesem Zusammenhang spielt auch die Vorschrift des § 32 e Abs. 2 Ziff. 2 BDSG-E eine Rolle, die ebenfalls in rechtsstaatlich bedenklicher Weise ausdrücklich die heimliche Erhebung von Daten zur Verhinderung von Straftaten oder schwerwiegenden Pflichtverletzungen – also ebenfalls im präventiven Bereich – bei einzelnen Beschäftigten zulässt.

Wie unbestimmt das Verhältnis von Aufklärung begangener Rechtsverstöße einerseits und der Verhinderung zukünftiger Rechtsverstöße andererseits ist, belegen auch die „Formulierungsvorschläge“ des Bundesministeriums der Justiz vom 07.09.2011, wonach Datenscreenings – entgegen dem Wortlaut des Gesetzentwurfs vom 15.10.2010 („zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen“) – nun doch auch "zu deren Vermeidung" vorgesehen werden sollen, was eine Rückkehr zum Referentenentwurf des BMI vom 28.05.2010 darstellt. In diesem Formulierungsvorschlag liegt ein deutliches Einfallstor für die Ausweitung der gesetzlichen Prüf- und Kontrollpflichten des Arbeitgebers im Bereich der Compliance und damit die Gefahr einer Ausweitung des Anwendungsbereichs des § 130 OWiG. Einer solchen sanktionsbewehrten Inpflichtnahme des Arbeitgebers ist entschieden zu widersprechen. Nicht ohne Grund existieren Sonderregelungen im KWG und im WpHG für erhöhte Prüf- und Kontrollpflichten, deren Ausweitung über das Bundesdatenschutzgesetz auf sämtliche Arbeitgeber sich verbietet.

Präventive, flächendeckende Screenings von Beschäftigtendaten ohne konkreten Tatverdacht sind unzulässig. Eine kriminalpolitische Notwendigkeit, von der Rechtslage de lege lata abzuweichen, ist nicht ersichtlich. Die aktuelle Regelung des § 32 Abs. 1 S. 2 BDSG hat sich in der Praxis bewährt und gibt dem Arbeitgeber einen genau umrissenen Rahmen vor, der sich aus einem konkreten Anfangsverdacht, dessen Dokumentation sowie einer Verhältnismäßigkeitsprüfung bzw. Interessenabwägung zusammensetzt. Ob und inwieweit ein Datenscreening zulässig ist, ist nach geltender Rechtslage in § 32 Abs. 1 S. 2 BDSG klar, praktikabel und verhältnismäßig geregelt. Zudem ist zu berücksichtigen, dass es bereits nach geltender Rechtslage zulässig ist, durch die Auswertung von Vorgangsdaten besonders korruptionsgefährdete Problembereiche in Unternehmen zu lokalisieren, wenn eine Repersonalisierung der Daten nicht möglich ist und dem Gebot der Datenvermeidung und Datensparsamkeit (vgl. § 3 a BDSG) Genüge getan wird (Brink/Schmidt, MMR 2010, 592, 594). Ein solches Vorgehen macht ein flächendeckendes, dauerhaftes Massenscreening mit hoher Eingriffsintensität entbehrlich und genügt den Anforderungen an eine wirksame Compliance.

Schließlich ist auf folgenden Gesichtspunkt hinzuweisen:
Die Kosten- und Arbeitsbelastung für die Wirtschaft durch Compliance-Systeme ist schon nach geltender Rechtslage enorm. Die gestiegenen Anforderungen an Compliance-Systeme erfordern schon jetzt riesige Kapazitäten an Personal und finanzieller Ausstattung. Die Durchführung von zeitlich unbegrenzten, verdachtsunabhängigen und flächendeckenden Massenscreenings würde einen zusätzlichen finanziellen und personellen Aufwand erfordern, der von Unternehmen – gerade von kleinen und mittelständischen Unternehmen – kaum zu leisten wäre. Dies gilt insbesondere im Hinblick auf die Auswertung der Datenbestände, vor allem aber auch für die Gewährleistung der Anonymisierung, Pseudonymisierung sowie die Kontrolle und Dokumentation einer etwaigen Repersonalisierung.

h) Unklares Konkurrenzverhältnis zu den Spezialvorschriften gemäß §§ 25 c Abs. 2 KWG, 33 b Abs. 3 WpHG

In den §§ 25 c Abs. 2 S. 1, S. 2 KWG, 33 b Abs. 3 WpHG sind für Kreditinstitute verdachtsunabhängige Datenabgleiche vorgesehen. Die Gesetzesbegründung zu § 32 d Abs. 3 BDSG-E nimmt ausdrücklich auch auf Unternehmen der Kreditwirtschaft Bezug, was impliziert, dass die Vorschrift des § 32 d Abs. 3 BDSG-E auch auf Unternehmen der Kreditwirtschaft Anwendung finden soll. Damit versäumt es der Gesetzentwurf, die Anwendbarkeit der – zum Teil konkurrierenden – Regelungen zu bestimmen. Das Konkurrenzverhältnis der Vorschriften bleibt im Dunkeln. Die Rechtsunsicherheit kann nur verhindert werden, wenn der Gesetzgeber das Verhältnis der aufsichtsrechtlichen Vorschriften zu § 32 d Abs. 3 BDSG-E klar bestimmt und ggf. Sonderregelungen für Unternehmen in der Finanzwirtschaft schafft. Alternativ könnte – wie im Gesetzentwurf des Bundesrats vorgeschlagen (BR-Drucksache 535/10) – neben dem Straftatenkatalog auch ein Screening „zur Erfüllung gesetzlicher Prüf- oder Kontrollpflichten“ vorgesehen werden. Allerdings müssen auch Screenings im Finanzsektor den verfassungsrechtlichen Vorgaben genügen, so dass dauerhafte und automatisierte Screenings mit personenbezogenen oder personenbeziehbaren Daten zwingend unterbleiben müssen.

i) Keine Beweisverwertungsverbote

Schließlich ist zu bemängeln, dass die Vorschrift des § 32 d Abs. 3 BDSG-E keine Aussage zu Beweisverwertungsverboten im Falle eines unrechtmäßig durchgeführten Datenabgleichs trifft. So ergeben sich bereits nach der Rechtsprechung des BAG bei schweren Verstößen gegen datenschutzrechtliche Normen Beweisverwertungsverbote (vgl. dazu nur BArbG NJW 2008, 2732, 2733). Dennoch wäre es zur Klarstellung erforderlich gewesen, Verwertungsverbote zu normieren. Ein effektiver Schutz der Beschäftigten gegen Ausforschung und Bespitzelung ist nur dann gewährleistet, wenn sichergestellt ist, dass die Ergebnisse unzulässiger Datenabgleiche nicht verwertet werden. Dies gilt umso mehr, als die Vorschrift des § 28 Abs. 2 Ziff. 2 b) BDSG die Möglichkeit eröffnet, den erhobenen Datenbestand – auch schon im Vorfeld eines Anfangsverdachts – im Wege einer Zweckänderung den Ermittlungsbehörden zur Verfolgung von Straftaten zu übermitteln (vgl. hierzu Wehnert in: Kempf/Lüderssen/Volk (Hrsg.), Ökonomie versus Recht im Finanzmarkt?, S. 137, 142).

- - -