rischen Beitrags von *Stefan Ullrich*. „*Wenn wir das Individuum vor datenhungrigen Organisationen schützen wollen, müssen wir ihm das Sich-Organisieren-Können zugestehen. Wir, verehrte Anwesende, brauchen eine Datenwehr*“ ist das Fazit seines *Datenschutz-Konzils*, in dem Vertreter „*verschiedene[r] Stände, Ämter, Geschlechter und nicht zuletzt: Zeitalter*“ über das Thema verhandeln.

Das Spannungsfeld zwischen einem Datenschutzbegriff, der als umfassender Schutz des Persönlichkeitsrechts verstanden wird, und einem Datenschutzbegriff, der die (technische) Datensicherheit in den Mittelpunkt stellt, behandelt *Jörg Pohle*. Er sieht in *Datenschutz by Design* die Umdefinition des Datenschutzes in Datensicherheit, und damit den V
leme technisch zu lösen. „*Die Fo*
schreibt er, „*lassen sich bis heute*
beiten zur Technikgestaltung – u
schutzpraxis – beobachten: Gerade die Technikwissenschaften sind geprägt von Arbeiten, die IT security *als* privacy *und Daten*sicherheit *als Daten*schutz *verkaufen. Anstatt die modernen Organisationen und ihre Informationsverarbeitung unter Kontrolle zu bringen, geht es in erster Linie um Konzepte wie die Verschlüsselung von Kommunikation, die Anonymisierung erhobener und gespeicherter Informationen oder Selbstschutzmaßnahmen von Betroffenen, ohne zu reflektieren, ob diese Ansätze im konkreten Fall überhaupt geeignet sind, einen Schutz der Betroffenen sicherzustellen.*“

Einen Überblick über *Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google* gibt *Angela Meindl* in ihrem Beitrag *Internet-Profiling*. „*Die Art und Weise, wie vom Nutzer unbemerkt Daten über ihn erhoben und gespeichert werden, ist nicht akzeptabel. Mit welcher Begründung auch immer sie gerechtfertigt wird. Ohne Notwendigkeit muss jeder, der an dieser Gesellschaft teilhaben will, auf seine Privatsphäre verzichten, und trägt ein nicht zu unterschätzendes Gefährdungsrisiko, während diejenigen, die für diesen Zustand verantwortlich sind, Unmengen Geld mit unserer Privatsphäre verdienen*“, so ihr Resümee. Sie fordert ein internationales Datenschutzrecht und dessen konsequente Kontrolle und Durchsetzung.

Wer bisher meinte, mit dem Berechtigungskonzept von Android datenhungrige Apps erkennen und aussperren zu können, erlebt nach der letzten Umgestaltung zu Berechtigungsgruppen eine böse Überraschung. Dies und anderes thematisiert *Carsten*
id? Aber sicher!?, der auch wie-
itteln sich eine scheinbar berech-
Kontrolle über das eigene Smart-

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Weitere Beiträge zum Thema gibt es in der Rubrik *Retrospektive* mit dem Artikel *Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten*, in dem *Ulrich Seidel* 1970 den modernen Begriff des Datenschutzes prägte, und in der Rubrik *Lesen & Sehen*, in der *Marie-Theres Tinnefeld* den Band *Finger weg von unseren Daten* von *Jan Philipp Albrecht* rezensiert.

Wir hoffen, mit unserem Schwerpunkt interessante Perspektiven auf das komplexe Thema Datenschutz zu geben, und wünschen eine erkenntnisreiche Lektüre.

Die Schwerpunktredaktion
Stefan Hügel, Eberhard Zehendner

Lutz Hasse

Datenschutz in Thüringen – es bleibt spannend!

A. Am Anfang war – das Bundesverfassungsgericht

„Datenschutz“ wird zumeist als Synonym gebraucht für das Grundrecht der informationellen Selbstbestimmung. Dieses Grundrecht wurde bereits 1983 vom Bundesverfassungsgericht in seinem berühmten Volkszählungsurteil aus der Taufe gehoben (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83) und mit der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008 (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07) zu dem weiteren Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme fortentwickelt und optimiert. Die Weitsicht des Volkszählungsurteils wird unter anderem in folgenden Passagen deutlich (BVerfGE a.a.O., Rz. 148, 149, 152 zitiert nach juris):

> *„Mit dem Recht auf informationelle Selbstbestimmung wäre eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.“*

> *„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“*

> *„Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum mehr.“*

B. Verfassungsrechtliche Grundlagen

Die Vorgaben des Volkszählungsurteils haben ihren Niederschlag in Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen gefunden:

> *„Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen."*

Was aber sind personenbezogene Daten? Hier hilft der Gesetzgeber weiter. Nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) – das insbesondere für Thüringer Behörden gilt – sowie nach § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) – das insbesondere für Unternehmen gilt – sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Aufmerksamkeit verdient die „bestimmbare" Person. Denn anders als bei Einzelangaben, die unmittelbar auf eine bestimmte Person schließen lassen (Name, Telefonnummer, Anschrift, E-Mail-Adresse), genügen hinsichtlich einer bestimmbaren Person solche Einzelangaben, die erst unter Hinzuziehung weiterer Angaben die hinter diesen Angaben stehende natürliche Person erkennen lassen. Also bereits Informationsmosaiksteinchen, die nur in Verbindung mit weiteren Mosaiksteinchen ein Bild von einer erst dann bestimmbaren Person ergeben können (zum Beispiel IP-Adresse in Verbindung mit weiteren Informationen), sind personenbeziehbar und damit personenbezogen und vom Grundrecht der informationellen Selbstbestimmung geschützt.

Indes ist dieser Schutz nicht absolut. Denn wie auch schon im Volkszählungsurteil angelegt, sieht Art. 6 Abs. 3 der Verfassung des Freistaates Thüringen vor, dass das Grundrecht der informationellen Selbstbestimmung auf Grund eines Gesetzes eingeschränkt werden darf.

C. Das Verbot mit Erlaubnisvorbehalt

Diese Möglichkeit, das Grundrecht der informationellen Selbstbestimmung aufgrund eines Gesetzes einzuschränken, ist in § 4 Abs. 1 ThürDSG/BDSG konkretisiert. Danach ist eine Datenverarbeitung und Datennutzung von personenbezogenen Daten nur zulässig, soweit das ThürDSG/BDSG oder eine andere Rechtsvorschrift es erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Juristen nennen das *Verbot mit Erlaubnisvorbehalt*: Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist grundsätzlich verboten. Eine Ausnahme besteht nur dann, wenn es eine *ausdrückliche gesetzliche Regelung* dafür gibt oder die Betroffenen in die Verarbeitung ihrer Daten *eingewilligt* haben.

Unter Datenverarbeitung ist dabei das Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten zu verstehen (§ 3 Abs. 3 ThürDSG). Wichtig: Für jede der zuvor erwähnten Aktionen ist eine Einwilligung oder Rechtsgrundlage erforderlich! Unter einer *Einwilligung* wird die auf *freiwilliger* Entscheidung beruhende Willenserklärung des Betroffenen verstanden, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen (§ 4 Abs. 2 ThürDSG, § 4a Abs. 1 BDSG). In der Regel bedarf die Einwilligung der Schriftform (vgl. § 4 Abs. 3 S. 2 ThürDSG, § 4a Abs. 1 S. 2 BDSG).

Mithin ergibt sich bei Datenschützern im Falle einer Verarbeitung personenbezogener Daten folgender Gedankengang:

1. Liegt eine Einwilligung vor?

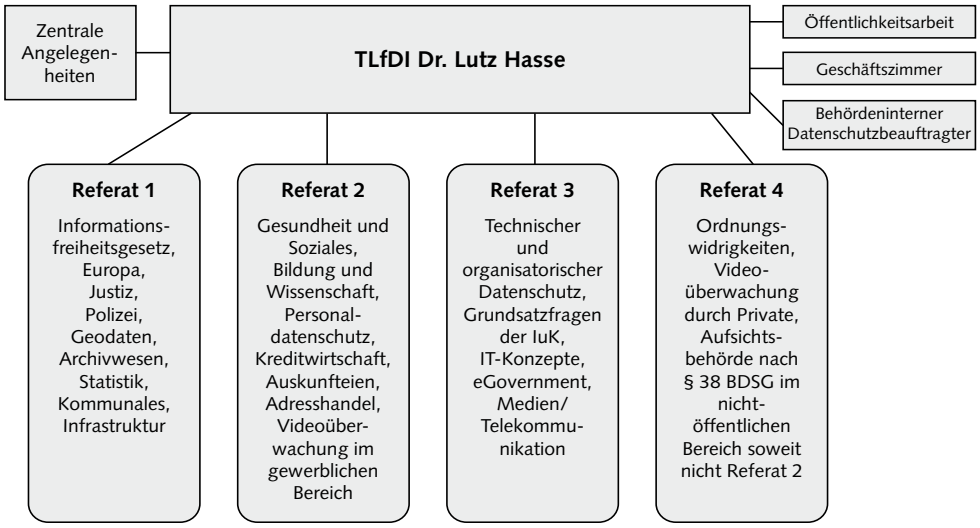
Falls nein:

2. Erlaubt eine Rechtsvorschrift die Datenverarbeitung?
   a. Spezielles Gesetz (z. B. Polizeigesetz, Schulgesetz, Sozialgesetzbuch)?
      Falls nein:
   b. Allgemeines Gesetz (ThürDSG, BDSG)?
      Falls nein:
      Datenverarbeitung ist rechtswidrig!

      Falls ja (a oder b):
      Datenverarbeitung ist rechtmäßig, wenn das Gesetz verfassungskonform ist und die vom Gesetz aufgestellten Voraussetzungen erfüllt sind.

D. Wir über uns

Die Abkürzung TLfDI steht für den *Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit*. Der TLfDI wird für sechs Jahre vom Landtag gewählt. Seit dem 29. Dezember 2012 ist er auch Beauftragter für die Informationsfreiheit im Freistaat Thüringen. Er übt diese Funktionen in völliger Unabhängigkeit aus und wird von einem engagierten Team unterstützt. Das nachfolgende Organigramm gibt Informationen zu den Aufgaben und dem Aufbau der Behörde. Weitere Infos dazu finden sich auf der Internetseite des TLfDI *(www.tlfdi.de)* unter dem Link: *http://www.tlfdi.de/tlfdi/wir/dienststelle/*.



Organigramm des TLfDI

E. Einblicke in die Tätigkeiten des TLfDI im öffentlichen Bereich (Behörden)

Der Bereich der Polizei beschäftigte den TLfDI in den vergangenen Jahren in besonders starkem Maße. Zu nennen ist die datenschutzrechtliche Begleitung des Papstbesuches, da mit diesem Ereignis zahlreiche Datenerhebungen im Vorfeld und während der Veranstaltung verbunden waren. Im sogenannten „Toilettenpapierfall" musste der TLfDI eingreifen, weil die Beschäftigten des Thüringer Landeskriminalamtes aufgrund des Verdachts des Abhandenkommens von Toilettenpapier videoüberwacht wurden. Auch gab es Fälle, in denen Polizeibeamte durch ihre Kollegen „ausspioniert" wurden. Da den TLfDI in der Vergangenheit die vielfach komplexen und mitunter recht unebenen „Regelungslandschaften" der Aufbewahrungs- und Prüffristen bei den öffentlichen Stellen beschäftigten, erarbeitete er den umfangreichen Leitfaden „Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut beim Thüringer Landesamt für Verfassungsschutz, in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften". Hierbei wurden alle einschlägigen Regelungsmaterien im Zusammenhang dargestellt und erläutert. Ein weiterer Schwerpunkt war die Fortführung der Kommunalkontrollen. Es bestand zudem der Verdacht, dass die in der Thüringer Landesverwaltung verwendeten Telefonanlagen über eine sogenannte „Babyphone-Funktion" verfügten, die es technisch ermöglichten, einen Raum zu überwachen.

Beleuchten wir nun einige der oben erwähnten Fälle aus dem öffentlichen Bereich näher:

1. Klopapier – Thüringer Landeskriminalamt von der Datenschutz-Rolle

Aufgrund von Medienberichten wurde dem TLfDI bekannt, dass das Thüringer Landeskriminalamt (TLKA) verdeckte Videoaufnahmen angefertigt hatte. Auslöser für die Ermittlungen war das unerklärliche Verschwinden von Toilettenpapierrollen – der Verdacht eines Diebstahls lag in der Luft. Um den Dieb zu finden, installierten Überwachungsspezialisten des TLKA eine Videokamera in einem Flur unweit der Toiletten, wo die Toilettenpapierrollen in Liefersäcken gelagert wurden. Ziel war es, einen möglichen Täter bei der Entwendung des angeblich so begehrten Toilettenpapiers zu überführen. Selbst nach wochenlanger Überwachung konnte kein Täter ermittelt werden. Auch die inzwischen eingeschaltete Staatsanwaltschaft stellte das Verfahren ergebnislos wieder ein.

Die datenschutzrechtliche Prüfung dieses Falles durch den TLfDI erwies sich zeitweise als schwierig, da die angeforderten Unterlagen vom TLKA nicht an den TLfDI übermittelt wurden. Die mangelnde Unterstützung seitens des TLKA wurde vom TLfDI gemäß § 39 ThürDSG beanstandet.

Die heimlichen längerfristigen Videoaufzeichnungen stellten zudem eine Verletzung des informationellen Selbstbestimmungsrechts dar, soweit sich Personen tatsächlich durch den Aufnahmebereich der Videokamera bewegt hatten. Denn eine Rechtsgrundlage, die hier die Fertigung der heimlichen Videoaufzeichnungen legitimieren konnte, war nicht vorhanden. Aus Sicht des TLfDI handelte es sich hier um eine Observation, die grundsätzlich nur durch ein Gericht angeordnet werden darf (§ 163f Abs. 3 StPO – Längerfristige Observation). Eine solche Anordnung lag hier jedoch nicht vor. Darüber hinaus waren die Videoaufzeichnungen auch nicht verhältnismäßig. Die konkrete Videoüberwachung konnte an sich schon nicht zur eindeutigen Überführung des Täters beitragen und war daher ungeeignet. Denn eine Entnahme der Toilettenpapierrollen aus dem Plastiksack im Flur hätte zunächst nicht geheißen, dass dieses auch gestohlen werden sollte. Selbst wenn eine Toilettenpapierrolle in Zueignungsabsicht entwendet worden wäre, hätte das keine Rückschlüsse auf den Dieb hinsichtlich der in den Toilettenräumen befindlichen Papierrollen zugelassen. Als milderes Mittel hätte man z. B. weniger Toilettenpapierrollen in die Toilettenräume legen bzw. zeitweise kontingentieren oder abschließbare Toilettenpapierrollenhalter anschaffen können. Zudem stand die Maßnahme außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts. Festgestellt wurde hier lediglich ein hoher Verbrauch von Toilettenpapier im TLKA. Was diesen mysteriösen Verbrauch jedoch verursachte, konnte nicht ermittelt werden. Die datenschutzrechtlichen Verletzungen hat der TLfDI nach § 39 Abs. 1 ThürDSG beanstandet.

2. Babyphone im Dienstzimmer: Wozu?

Wer kennt das nicht: Plötzlich knackt es komisch im Telefon oder die Verbindung wird gefühlt irgendwie schlechter. Auch erscheint es manchen komisch, dass der Chef von Dingen weiß, die man anderen, aber nicht ihm erzählt hat. Hört der Chef etwa heimlich mit? Die Aufschaltfunktion bei einer Telekommunikationsanlage kann dazu missbraucht werden, dass zum einen bei geführten Telefonaten Dritte unbefugt mithören können und zum anderen bei der ebenso vorhandenen sogenannten Babyphone-Funktion – obwohl gar nicht telefoniert wird in dem Raum, in dem sich der Telefonapparat befindet – alles mitgehört werden kann. Aus datenschutzrechtlicher Sicht stellt das Ab- oder Mithören von Telefongesprächen oder Gesprächen im Raum eine Erhebung personenbezogener Daten dar. Die Verarbeitung einschließlich Erhebung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Aufgrund der Bedeutsamkeit des Themas wandte sich der TLfDI an alle Behörden der Thüringer Landesverwaltung, an die Kommunen und die kreisfreien Städte sowie auch an die Thüringer Handwerkskammern und die Industrie- und Handelskammern Thüringens und informierte die Stellen über diese datenschutzrechtliche Gefahr. Nicht nur die Dienstherren müssten die Leistungsmerkmale ihrer Telekommunikationsanlagen regelmäßig auf Rechtmäßigkeit prüfen. Auch Personalräte und Betriebsräte sollten die möglichen und tatsächlich eingestellten Leistungsmerkmale der Telekommunikationsanlagen regelmäßig hinterfragen. Der TLfDI konnte konkrete Verstöße nicht feststellen, immerhin aber, dass derartige Funktionen bestehen, die jedoch auch aufgrund der Aktivitäten des TLfDI deaktiviert wurden. Wir bleiben dran!

3. Abgeordnete des Thüringer Landtags zu Unrecht im Fokus der Polizei

In einer polizeilichen Ermittlungsakte stellte der TLfDI fest, dass sich dort personenbezogene Daten von Abgeordneten des Thü-

ringer Landtags befanden. Diese gelangten in die Ermittlungsakten, da im Rahmen einer Durchsuchung bei einem Beschuldigten auch sein privates Smartphone sowie Datenträger sichergestellt und ausgewertet wurden. Auf diesen befanden sich unter anderem auch die Daten der Abgeordneten. Eine Einwilligung zur Datenverarbeitung seitens der Abgeordneten lag nicht vor. Als Alternative zur Einwilligung käme die Existenz einer speziellen Rechtsgrundlage in Betracht, die aber auch hier nicht vorgelegen hatte. Abgeordnete des Thüringer Landtags sind nach § 53 Abs. 1 Satz 1 Nr. 4 Strafprozessordnung (StPO) berechtigt, das Zeugnis zu verweigern. Daher war hier auch der § 160a StPO zu beachten. § 160a Abs. 1 StPO bestimmt zunächst, dass eine Ermittlungsmaßnahme, die sich gegen eine zeugnisverweigerungsberechtigte Person (hier: die Abgeordneten des Thüringer Landtags) richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig ist. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Nach § 160a Abs. 1 Satz 5 StPO gilt dies darüber hinaus entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine zeugnisverweigerungsberechtigte Person (Abgeordnete) – also einen Dritten – richtet, über diese Person (Abgeordnete) Erkenntnisse erlangt werden, über die sie (Abgeordnete) das Zeugnis verweigern dürfte. Im vorliegenden Sachverhalt erfolgte nach Aufnahme der Daten der Abgeordneten in die Ermittlungsakte eine – wie vom Gesetz vorgeschrieben – unverzügliche Löschung der Daten jedoch nicht. Der TLfDI hat dies gemäß § 39 ThürDSG beanstandet, da hier ein ungerechtfertigter Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Abgeordneten zu sehen war.

4. Polizei auf Abwegen

Die Staatsanwaltschaft Mühlhausen ermittelte gegen Polizeibeamte wegen des Verdachts des Betrugs und der Untreue. Hintergrund war eine anonyme Anzeige gegen vier namentlich benannte Tatverdächtige. Ihnen wurde vorgeworfen, dienstliche Kraftfahrzeuge und Telekommunikationsmittel während der Dienstzeit privat genutzt zu haben. Das zuständige Amtsgericht erließ auf Antrag der Staatsanwaltschaft einen Beschluss für eine längerfristige Observation gemäß § 163f Strafprozessordnung (StPO) gegen die vier Beschuldigten. Da für die längerfristige Observation der vier Beschuldigten nach § 163f StPO eine richterliche Anordnung vorlag, war eine rechtliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben und datenschutzrechtlich nicht zu beanstanden. Darüber hinaus wurden jedoch im Zuge der Observationsmaßnahmen drei weitere Polizeibeamte gezielt „mit-observiert“, von denen man vage annahm, dass auch diese die Dienstwagen privat genutzt hätten. Dazu wurde die ursprüngliche richterliche Anordnung einfach „geschwärzt“. Eine solche „geschwärzte“ Anordnung, die quasi als richterliche Blankoanordnung für sämtliche Observationsmaßnahmen verwendet wurde, stellt jedoch keine rechtliche Grundlage dar, auf die eine längerfristige Observation gestützt werden kann.

Im Übrigen waren auch die Voraussetzungen für eine kurzfristige Observation einschließlich Fotodokumentationen gemäß §§ 161 Abs. 1, 163 Abs. 1 i. V. m. § 100 h StPO nicht erfüllt. Zwar ist für kurzfristige Observationsmaßnahmen und in diesem Zusammenhang auch für die Herstellung von Lichtbildern keine richterliche Anordnung vorgesehen, dennoch muss auch hier der Anfangsverdacht begründet sein; eine bloße Vermutung genügt – wie hier – nicht.

Durch den Einsatz heimlicher Observationsmaßnahmen ohne rechtliche Grundlage wurde intensiv in das Recht auf informationelle Selbstbestimmung der drei weiteren betroffenen Personen eingegriffen. Diese erhebliche datenschutzrechtliche Verletzung hat der TLfDI förmlich nach § 39 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet.

F. Einblicke in die Tätigkeit des TLfDI im nichtöffentlichen Bereich (insbesondere Unternehmen)

Zur Einstimmung:

Dashcam – Trashcam

Auto, Fahrrad, LKW;
die Dashcam ist dabei – oje.
davor, dahinter, nebendran,
Personen, Unfall, Autobahn,
Dashcam zeichnet's auf – ein Wahn.

Tatsächlich, und da herrscht Einigkeit,
verfehlt sie die Datenschutz-Zulässigkeit.
Zwar sind schon von Gesetzes wegen
Ausnahmetatbestände vorgegeben,
die Filmen in Familienkreisen
sowie auch von privaten Reisen,
dem Bundesdatenschutz entreißen.

Dashcams muss man,
das sollte man wissen,
nach dem BDSG besser doch missen.
Das Filmen von Unfällen, eigenen – fremden,
um das dann vor Gericht zu verwenden,
ist keine persönliche Tätigkeit,
die vom Anwendungsbereich befreit.

Vom Filmen von öffentlichen Räumen,
darf der Einzelne nur träumen,
es sei denn, man hat das Hausrecht inne
und dieses dabei auch im Sinne.
Ebenfalls, so die Gesetze,
kann aus berechtigtem Interesse
dann aber nur zu bestimmtem Zwecke
die Kamera an des Hauses Ecke.

Darüber hinaus, man glaubt es kaum,
sind schutzwürdige Interessen im Raum.
Erst wenn keine Punkte vorliegen,
dass diese Interessen überwiegen,
wird es mit der Filmerei
mehr als nur `ne Träumerei.

Beim Autofahren, so sei bedacht,
ist Kamera nicht angedacht,
so liegt es nach Natur der Dinge,

auf der Straße wird's mit dem Hausrecht dünne.
Zwar sind fürs Filmen die eig'nen Interessen
des Autofahrers nicht sogleich vermessen,
doch beim Aufnehmen anderer im Verkehr,
ist für jeden erkennbar gar nicht schwer,
dass Anhaltspunkte sind vorhanden
für's Überwiegen der Interessen der and'ren,
nämlich gerade auch der Passanten.

Wegen des hier Erreimten sei dem Bürger gesacht,
dass der Datenschützer über den Datenschutz wacht.
Der Verstoß, wie grade berichtet,
wird gern mit Bußgeldern gerichtet.
Daher hier noch ein letzter Satz:
Lieber Besitzer einer Dashcam,
diese gehört ganz schnell in die „Trashcan"!

Es sind bereits Urteile zur Dashcam ergangen. So das Urteil der 4. Kammer des Verwaltungsgerichts Ansbach vom 12. August 2014 (AN 4 K 13.01634). Der Kläger wandte sich im vorliegenden Verfahren gegen einen Bescheid, mit welchem ihm untersagt worden war, mit der im Fahrzeug des Klägers eingebauten On-Board-Kamera während der Autofahrt permanente Aufnahmen des vom Kläger befahrenen öffentlichen Bereichs zu machen. Zugleich wurde dem Kläger aufgegeben, Aufnahmen, die mit der Kamera gemacht wurden, zu löschen. Maßgebend hierfür ist, dass das Bundesdatenschutzgesetz heimliche Aufnahmen unbeteiligter Dritter grundsätzlich nicht zulässt und diese einen erheblichen Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung darstellen. Das Interesse betroffener Personen überwiegt deshalb das geltend gemachte Interesse des Klägers an der Fertigung von Aufnahmen mit einer Dashcam. Videoaufnahmen dürfen nicht ohne Zustimmung der Gefilmten angefertigt werden, wenn sie den Zweck haben, an Dritte weitergegeben zu werden. Dazu zählt neben der Veröffentlichung im Internet auch die Weitergabe an die Polizei. Der gesetzlich festgelegte Bußgeldrahmen für derartige Verstöße beläuft sich auf bis zu 300.000 EUR. Im jüngsten Urteil vom 23. April 2015 hat das Amtsgerichts Nienburg (4 Ds 155/14) erstmals eine Dashcam-Aufnahme für einen Strafprozess als Beweismittel zugelassen. Jedoch mit der Einschränkung, dass die Aufnahme aus aktuellem und konkretem Anlass erfolgen muss: In diesem speziellen Fall hat der Zeuge die Dashcam nur zur Dokumentation einer Nötigung im Straßenverkehr aufgenommen. Anders verhält es sich, wenn man die Dashcam dauerhaft aktiviert. Hier trifft wieder das o. g. Urteil des Verwaltungsgerichts in Ansbach zu, dass der Einsatz von Dashcams unter bestimmten Umständen gegen den Datenschutz verstößt. Diese Meinung vertritt auch der TLfDI.

1. Feuermelder mit Augen

Über einen anonymen Hinweisgeber wurde dem TLfDI der Tipp gegeben, dass ein Arbeitgeber in der Umkleidekabine seines Unternehmens mit angeschlossenem Duschraum eine verdeckte Videoüberwachung mit Audiofunktion – getarnt als Rauchmelder – durchführen würde. Am Folgetag hat der TLfDI vor Ort kontrolliert. Nachdem man den TLfDI widerwillig auf das Betriebsgelände ließ, musste festgestellt werden, dass der entsprechende Umkleideraum über Nacht umfassend renoviert worden war. Es roch sogar noch nach frischer Farbe. Im darauf folgenden Verwaltungsverfahren konnte festgestellt werden, dass der Arbeitgeber mit der Videokamera Einbrüche in die Spinde seiner Arbeitnehmer aufklären wollte. Die Kamera war direkt nach einem Einbruch installiert worden. Insgesamt wurde die Kamera etwa zwei Wochen betrieben. In diesem Zeitraum kam es erneut zu einem Einbruch. Die Auswertung der Überwachung ermittelte den Täter, ihm wurde gekündigt. Was vorbildlich klingen mag, ist es leider manchmal nicht, so auch in diesem Fall. Auch wenn aus Sicht des Arbeitgebers alles wunderbar geklappt hat, sind im Bereich des Arbeitsverhältnisses datenschutzrechtliche Vorschriften zu beachten. Nicht alles, was zweckmäßig erscheint, ist auch zulässig. Zwar sieht § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) explizit die Datenerhebung zu Zwecken der Aufklärung von Straftaten im Beschäftigungsverhältnis vor, jedoch sind diese nur unter besonderen Voraussetzungen zulässig. Dabei fließt mit ein, dass eine Videoüberwachung in einem Umkleideraum anders zu bewerten ist als eine Videoüberwachung in einem Kassenbereich. So darf eine heimliche Videoüberwachung nur dann durchgeführt werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Bereits der letzte Punkt war in dieser Konstellation nicht gegeben. Eine verdeckte Videoüberwachung in einem Umkleideraum, der für eine Komplettentkleidung vorgesehen ist, ist fast immer unverhältnismäßig, da hier in einem Maße in die Intim- und damit Persönlichkeitssphäre der Betroffenen eingegriffen wird, die eine Abwägung zu Gunsten der Interessen des Überwachenden fast unmöglich macht. Darüber hinaus wurden in diesem Fall jedenfalls nicht alle anderen Mittel zur Aufklärung ausgeschöpft. Ein Ordnungswidrigkeitenverfahren wurde eingeleitet.

2. Nackt bis auf die Haut – saunieren und (unfreiwillig) posieren

Eine Gemeinde installierte in dem Saunabereich ihres Hallenbads Videokameras, mit denen sowohl eine Videobeobachtung als auch eine Videoaufzeichnung erfolgten. Als Grund für die Bildaufzeichnungen führte die Gemeinde an, dass zum einen Diebstähle damit vermieden werden sollten und zum anderen, dass die Bademeister hätten erkennen können, ob jemand einen Herzinfarkt im Saunabereich erleidet und so ein schnelles Eingreifen ermöglicht würde. Eine Einwilligung seitens der Saunabesucher lag jedoch nicht vor. Eine verdachtsunabhängige Videoüberwachung, insbesondere, wenn die Aufnahmen gespeichert werden sollen, stellt einen nicht unerheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und bedarf daher einer Rechtsgrundlage, die diesen Eingriff erlaubt. Es stellte sich die Frage, ob die Videoüberwachung zur Wahrnehmung des Hausrechts nach § 6 b Abs. 1 Nr. 2 BDSG zulässig war. § 6 b Abs. 1 Nr. 2 BDSG besagt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen

der Betroffenen überwiegen. Dies musste hier jedoch verneint werden. Das Hausrecht berechtigt zwar, Personen von Rechtsverstößen abzuhalten, dafür müssen aber konkrete Anhaltspunkte vorliegen, dass Rechtsverstöße in der Vergangenheit bereits begangen worden sind. Das war hier jedoch nicht der Fall. Als weitere Möglichkeit stellte sich die Frage, ob die Videoüberwachung zur Wahrnehmung berechtigter Interessen gemäß § 6 b Abs. 1 Nr. 3 BDSG gerechtfertigt werden konnte. § 6 b Abs. 1 Nr. 3 BDSG besagt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig ist, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In diesem Sachverhalt lagen jedoch keine objektiven Anhaltspunkte vor, dass der bestimmte Saunabereich, der videoüberwacht wurde, besonders gefährlich war. Zum anderen überwogen die schutzwürdigen Interessen der Saunabesucher an einer unbeobachteten Nacktheit die Interessen der Saunabetreiber. Ein regelmäßiger Rundgang des Bademeisters hätte in diesem Fall als milderes Mittel im Gegensatz zu einer Videoüberwachung ausgereicht. Wäre eine Person tatsächlich bewusstlos geworden oder hätte einen Herzinfarkt erlitten, könne davon ausgegangen werden, dass andere Saunabesucher sofort Hilfe geholt hätten. Die Videoüberwachung war somit rechtswidrig.

3. Finger von der Wurst!

Ein Landwirt hatte sich mehrere Hofläden zugelegt. Allerdings nahm er es mit der Sicherung seiner Produkte etwas zu ernst. Um sein Eigentum zu schützen, in diesem Falle ging es um die Wurst, schreckte er vor moderner Überwachungstechnik nicht zurück. So installierte er nahezu flächendeckend in allen Räumen Videokameras. In einer seiner Filialen war gar der einzige unbeobachtete Ort die Arbeitnehmertoilette. Er wollte damit verhindern, dass die hungrigen Verkäuferinnen sich ungehemmt hinter seiner Verkaufstheke bedienen können. Mit dem Bundesdatenschutzgesetz (BDSG) ist eine solche Videoüberwachung von Arbeitnehmern und Kunden selbstverständlich nicht zu vereinbaren. Zwar sieht das BDSG die Möglichkeit der Datenerhebung zu Aufklärung von Straftaten im Arbeitsverhältnis vor, jedoch nur in sehr engen Grenzen und vor allem in verhältnismäßigem Rahmen. Jedenfalls muss eine solche Videoüberwachung das allerletzte Mittel sein. Vorher muss z. B. bei einem Diebstahlverdacht eine Taschenkontrolle unter Heranziehung der örtlichen Polizei erfolgen. Die Kameras waren jedenfalls zu entfernen. In diesem Fall musste der TLfDI die Einhaltung des BDSG nicht mit Hilfe einer Anordnung durchsetzen. Der Bauer hatte kurz zuvor die Kameras nebst Kabel aus Zorn über den TLfDI aus den Wänden gerissen. Zielführend …

4. Übermittlung von Patientendaten an „Herrn Dr. *med.* Hasse“

Der TLfDI, Herr Dr. *jur.* Hasse, erhält zu Hause Post: Ein Krankenhaus in Thüringen übersendet verschiedene Arztberichte an „Herrn Dr. *med.* Hasse“. Die Nachfrage im Krankenhaus ergab: Die Anschrift des eigentlich gesuchten Arztes ähnlichen Namens war nicht im Krankenhausinformationssystem eingetragen. Das Krankenhauspersonal „recherchierte“ also nach der Anschrift im Internet. Das war rechtskonform. Das Krankenhaus muss jedoch nach § 9 BDSG alles tun, damit seine Mitarbeiter bei der Verarbeitung von Patientendaten die datenschutzrechtlichen Vorgaben einhalten. Hierzu gehört zum einen, alle technischen Anlagen so zu konzipieren, dass Unbefugte keinen Zugriff haben. Zum anderen muss durch organisatorische Maßnahmen, zum Beispiel durch Dienstanweisungen, sichergestellt werden, dass die sensiblen Daten nicht in falsche Hände geraten. Es muss daher eine schriftliche Anweisung geben, wie nach den Adressen gesucht wird und wie die Gesundheitsdaten übermittelt werden dürfen, die der Schweigepflicht unterliegen. Die Übermittlung der Gesundheitsdaten war somit rechtswidrig. Der Umstand, die Patientendaten ausgerechnet an den Landesdatenschutzbeauftragten gesendet zu haben, löste dann im Krankenhaus auch „heilsame“ Prozesse aus!

G. Zukunft? Ungewiss!!

Die zuvor unter E. und F. dargestellten Einzelfälle aus der Praxis des TLfDI mögen einen gewissen Spaßfaktor beinhalten, dürfen indes den Blick auf die generellen Gefahren für das Grundrecht der informationellen Selbstbestimmung nicht verstellen.

Soziale Netzwerke sollten entschleiert werden. Nutzer müssen über das Geschäftsmodell aufgeklärt werden sowie darüber, wie man dort sein Recht auf informationelle Selbstbestimmung einigermaßen schützen kann.

Lutz Hasse

Dr. **Lutz Hasse** legte die Juristischen Staatsexamina in Niedersachsen ab. Es folgten Assistenzen an der Universität Osnabrück und ab 1992 an der Friedrich-Schiller-Universität Jena. Die Promotion erfolgte während der „Jenenser Phase“ an der Universität Osnabrück. Anschließend erfolgte der Wechsel zur Thüringer Verwaltungsfachhochschule – Fachbereich Polizei; dort wurde er Leiter der Rechtsausbildung. Nach Tätigkeiten als Referatsleiter im Thüringer Innenministerium, beim Thüringer Landesbeauftragten für den Datenschutz und im Thüringer Sozialministerium wurde er 2012 vom Thüringer Landtag zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

Smart – Vorsicht! Smart suggeriert etwas Positives. Smart meters, smart grids, smart car, smart home, smart factory (Industrie 4.0), smart city, etc. Das Smarte daran ist, dass Unmengen von personenbezogenen Daten erhoben und ausgewertet werden und daraus Persönlichkeitsprofile erstellt werden können. Warum? Jeder Mosaikstein zählt, um sich von dem Nutzer ein Bild machen zu können. Warum? Wer weiß das seit den Offenbarungen vom Edward Snowden schon! Smart watches zum Beispiel übermitteln Gesundheitsdaten. Mit anderen Körperanalysegeräten ist hier ein Milliardenmarkt entstanden. Nur durch den Verkauf der Geräte? Und der Daten! Daten werden auch an anderen Einrichtungen gesammelt: Videokameras, Paycards, Clouds (Vorsicht, wenn die Serverkette nicht nachvollziehbar ist), Spielzeug (Xbox, Smartglasses, Fernseher, Puppen …). Und im Internet der Dinge könnte ein smarter Stromzähler bei einem bestimmten Lampen-Schaltrhythmus den illegalen Cannabisanbau im Keller entlarven.

Big Data: Alle diese Daten werden zu Big Data – einer umfassenden Datensammlung, die mit Hilfe moderner Software zur Erstellung eines kompletten Persönlichkeits-, Sozial-, Bewegungsprofils genutzt werden kann. Dabei können Datensammlungen öffentlicher Stellen (z. B. Behörden) mit denen nicht-öffentlicher Stellen (z. B. Unternehmen) kombiniert werden. Findet das statt? Eine Antwort beginnt damit, dass Behörden sich der Unterstützung von Unternehmen bedienen können … Übrigens: Google speichert täglich das Tausendfache an Daten, die in allen Werken der US-Kongressbibliothek enthalten sind! Warum wohl?

Und dann die Algorithmen.

Was bei Big Data nicht unmittelbar ablesbar ist, wird mit Hilfe von algorithmisch-mathematischen Formeln prognostiziert.

Beispiele: Predictive Policing: Aufgrund von Big-Data-Analysen werden Straßen, Gruppen und Individuen überwacht, weil sie für die Verbrechensbegehung zu bestimmten Zeiten als relevant erachtet werden. Oder: Terroristen sollen mit spezieller Software anhand von Herzschlag, Atemfrequenz, Körpersprache und anderer physischer Faktoren ausfindig gemacht werden. Nur in den USA? Deutsche Landeskriminalämter testen bereits entsprechende Software. Blick in die Zukunft: Freiheitsstrafe aufgrund algorithmisch ermittelter, aber tatsächlich nicht begangener Straftat (vgl. Science-Fiction-Thriller „Minority Report" mit Tom Cruise)? Wir erkennen Entwicklungen, allerdings nur solche, die offenkundig werden – etwa die angedachte Kooperation der Schufa mit einer Hochschule zur Auswertung sozialer Netzwerke mit Blick auf die Kreditwürdigkeit von Bankkunden. Aber nicht genug: Auch Schwangerschaften werden inzwischen erkannt – die Daten der Bankcards im Kaufhaus verraten es – mit Hilfe eines Algorithmus – Tag der Niederkunft inklusive!

Was kann man tun?

Staatliche Hilfe lässt seit den Enthüllungen von Edward Snowden leider zu wünschen übrig. Bürgerliche Selbsthilfe ist mithin von Nöten: Anonymes Surfen, Verschlüsselung, aktualisierte Sicherheitssoftware, Selbstfortbildung, berufliche Fortbildung, in sozialen Netzwerken die notwendigen Häkchen setzen, Widerspruchsrechte wahrnehmen, Datensparsamkeit im privaten Bereich, keine Bilder (!), Antivirensoftware für Smartphones, Sammlung der eigenen Daten – z. B. in sozialen Netzwerken – abfragen, ggf. „Löschung" bewirken.

Zudem: Fragen Sie Ihren Datenschutz-/Informationsfreiheitsbeauftragten!

Und warum überhaupt Schutz des Grundrechts?

Das Recht der informationellen Selbstbestimmung wurzelt in dem Grundrecht der Menschenwürde. Und zum Menschsein gehört das Recht, Geheimnisse zu haben. Sich nur insoweit zu offenbaren, wie wir es wünschen. Um zu entscheiden, welcher Mensch wir für andere Menschen sein wollen und welcher nicht. Um gemocht und respektiert zu werden.

Wissen wir, was wir tun?

Einer Studie zu Folge genügen bereits 10 Facebook-„Likes" einer Person, um sie besser einschätzen zu können als Arbeitskollegen es können, die immerhin 5 Tage pro Woche mit der Person zusammenarbeiten. Bei mindestens 70 „Likes" liegt der Computer mit seiner Einschätzung besser als Freunde und ab 150 „Likes" wird die Beschreibung der Persönlichkeit treffender als die von Familienangehörigen. Die höchste Hürde stellen Ehepartner dar. Um eine bessere Einschätzung der Persönlichkeit zu erreichen, werden mindestens 300 „Gefällt-mir"-Angaben benötigt. Kombiniert mit Daten von Handys, Videokameras, Einkäufen und Verbindungen zwischen den Individuen entstehen Datenkopien von der Realität. Mit der Option der sozialen Kontrolle. Durch wen? Den Staat? IT-Konzerne? Beide? Die Herren der Algorithmen gegen den Rest der Welt?

Maschinen, Roboter, PCs werden inzwischen lernfähig. Es entstehen echte kognitive Systeme, die nicht mehr nur Schach spielen. Die Fortschritte sind spektakulär. Die Maschinen beginnen, die Welt zu begreifen, sie lernen selbstständig, korrigieren ihre Fehler und interpretieren unvorstellbare Datenmengen.

Deep Learning heißt das Zauberwort. Der Einsatz von intelligenten Robotern wird – und das kann auch mit der modern klingenden Formel „Industrie 4.0" nicht beschönigt werden – nach neueren Prognosen bis nahezu 50 Prozent der Jobs gefährden. Natürlich entstehen auch Berufe im Umfeld der Entwicklung und Steuerung von Computersystemen. Rasch werden jedoch Übersetzer, Lagerarbeiter und Lastwagenfahrer ersetzt werden. Aber auch Journalisten und Rechtsanwälte. Ärzte werden in zunehmendem Maße unterstützt werden, aber ihre Domäne noch behaupten können. Berufe, die Empathie und soziale Kompetenzen verlangen, sind noch ungefährdet. Andererseits wird an Kranken- und Altenpfleger-Robotern bereits gearbeitet. Algorithmen können segensreiche Wirkungen entfalten, nicht nur in der Medizin. Aber auch die Gefahren sind unübersehbar. Wenn – was vorhersehbar ist – Roboter intelligenter sein werden als Menschen, welche Rolle werden sie einnehmen? Was passiert, wenn sich Algorithmen als fehlerhaft erweisen? Ist die Evolution selbst lernender Maschinen vom Menschen noch prognostizierbar? Kann künstliche Intelligenz mit menschlichen Werten wie Freude, Freiheit, Gerechtigkeit, Menschenwürde gefüttert

werden? Was, wenn das nicht gelingt und nur hochgezüchtete kühle künstliche Intelligenz den Ton angibt?

Der Mensch darf nicht zur Summe seiner Daten, nicht zum bloßen Produkt degradiert werden. Ohne unser Einverständnis darf ein digitales Ich weder generiert noch von Dritten mit einem Eigenleben versehen werden, das sich auf das reale Ich (negativ) auswirken kann. Die Autonomie ist die Grundlage unseres Menschseins. Dieser Autonomie hat die Transparenz der Datenverarbeitung zu dienen und nicht umgekehrt die Transparenz des Individuums der Aufblähung von Big Data. Transparenzgesetze – auch für Unternehmen – können Abhilfe schaffen. Die notwendige Stärkung der Selbstbestimmtheit gilt es zu fördern. Etwa durch gesetzliche Betonung des Einwilligungserfordernisses der Betroffenen vor einer Datenverarbeitung. Das Individuum muss in transparenter, umfassender und verständlicher Weise über die Verarbeitung seiner Daten informiert sein, bevor es eigenverantwortlich hierin einwilligt oder eben auch nicht.

Die informationelle Eigenverantwortung muss frühzeitig erlernt werden, auch in Kindertagesstätten und in der Schule. Medienkompetenz sollen Lehrkräfte vermitteln, die während ihrer Ausbildung auf das Schulfach Medienkunde vorbereitet wurden. Fortbildungsangebote müssen sich an der raschen Entwicklung im IT-Sektor ausrichten. Das schließt Informatik-Inhalte durchaus nicht aus. Evaluationen sind unabdingbar. Schließlich muss sich der Gesetzgeber anstrengen, Ballhöhe zu erlangen, damit der stets größer werdende Abstand zwischen Rechtslage und Realität nicht noch weiter auseinander klafft. Es darf nicht sein, dass die Privatsphäre torpedierende IT-Produkte aus wirtschaftlichen Gründen entwickelt werden (müssen), nur weil der Gesetzgeber nicht in der Lage zu sein scheint, derartige grundrechtswidrige Entwicklungen zu kanalisieren.

Wie geht es weiter?

Ist es mit dem Schutz des Grundrechts der informationellen Selbstbestimmung und der Privatsphäre ernst gemeint, müssen unabhängige Kontrollinstanzen die rasanten Entwicklungsprozesse begleiten – nachhaltig und effizient! Davon ist jedoch die Ausstattung der Datenschutzbehörden weit entfernt. Eines gerät leider zunehmend in Vergessenheit: Die Würde des Menschen ist unantastbar – nicht aber ein fragwürdiges Geschäftsmodell.

Eberhard Zehendner

Perspektiven des Datenschutzes

Jens Kubieziel und Eberhard Zehendner befragten am 8. April 2015 den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse.

Kubieziel: *Herr Dr. Hasse, können Sie uns kurz schildern, was der Inhalt Ihrer Tätigkeit ist, als Datenschützer und auch als Informationsfreiheitsbeauftragter.*

Hasse: Das sind eigentlich zwei Seiten einer Medaille. Als Datenschützer habe ich natürlich die Aufgabe, und die macht mir auch viel Freude, das Grundrecht der informationellen Selbstbestimmung der Bürger zu schützen. Und das Bundesverfassungsgericht hat ein weiteres Grundrecht hinzugefügt: die Vertraulichkeit und Integrität informationstechnischer Systeme. Das ist noch nicht so bekannt, fällt aber eben auch darunter.

Diese Grundrechte der Bürger schütze ich einmal, indem ich Behörden überwache und kontrolliere, ob sie die Datenschutzgesetze einhalten – was bisweilen nicht der Fall ist. Dann beanstande ich und wirke darauf hin, dass diese Lücken geschlossen, die Verstöße abgestellt werden.

Bei Unternehmen – da haben wir viel zu tun – habe ich mehr Möglichkeiten. Wenn dort Datenschutzverstöße festgestellt werden, kann ich Anordnungen treffen, bin also nicht nur Kontroll-, sondern auch Aufsichtsbehörde. Kann sagen, bauen Sie die Videokamera ab oder entlassen Sie Ihren Datenschutzbeauftragten. Wenn das nicht passiert, kann ich Zwangsgelder verhängen. Und wenn das immer noch nicht hilft, kann ich ein Bußgeld bis 300.000 Euro erlassen. Wir passen aber die Höhe des Bußgeldes der Stärke des Verstoßes und der finanziellen Leistungskraft des Unternehmens an.

Andererseits, als Informationsfreiheitsbeauftragter, habe ich dafür zu sorgen, dass Bürger Informationen von Behörden erhalten. Es gibt einen datenschutzrechtlichen Anspruch, dass der Bürger seine personenbezogenen Daten von der Behörde erhält. Es gibt jetzt aber auch einen Anspruch nach dem Thüringer Informationsfreiheitsgesetz, dass Bürger quasi alle Daten, die Behörden so haben, grundsätzlich bekommen können. Ziel ist, dass der informierte Bürger besser an demokratischen Prozessen teilhaben und gegenüber der Verwaltung eine gewisse Kontrolle ausüben kann. Das ist auch unmittelbar einleuchtend, finde ich.

Problem ist, dass dieses Gesetz gewisse Hürden enthält, die den Anspruch des Bürgers auf Information scheitern lassen. Etwa wenn öffentliche Interessen oder Urheberrechte gefährdet sind. Es gibt drei sehr lange Paragrafen, die für den Bürger Hürden aufbauen beim Zugang zu behördlichen Informationen. Diese Hürden müssen wir reduzieren, das wird im Koalitionsvertrag[1] auch zugesichert. Sehr ärgerlich ist, ein Unikum in der Bundesrepublik, dass ich als Informationsfreiheitsbeauftragter nicht kontrollieren darf, wenn Behörden sich auf einen Informationsverhinderungstatbestand berufen. Das ist absurd, das verstehen meine Informationsfreiheitsbeauftragtenkollegen aus anderen Ländern auch nicht, diese Vorschrift muss einfach gestrichen werden. Ich werde daher mit Hilfe meiner Mitarbeiter demnächst den Regierungsfraktionen sozusagen ein moderneres Informationsfreiheitsgesetz vorlegen.