

mung und Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme) sind von den ausländischen Geheimdiensten ignoriert worden; man hat den Eindruck, dass das, was technisch geht, auch gemacht wird. Jetzt muss entschlossen gehandelt werden, um die Souveränität zurückzugewinnen. Dazu gehören eine rasche europäische Datenschutzreform und die Aussetzung des Safe-Harbor-Abkommens, das bestenfalls nur noch symbolische Bedeutung hat. Außerdem sind im Transatlantischen Freihandelsabkommen (TTIP) gleiche Datenschutzstandards für Amerikaner wie Europäer auszuhandeln. Parallel dazu sind völkerrechtliche Abkommen zur Eindämmung von Geheimdienstaktivitäten erforderlich, weil das europäische Recht außereuropäische Geheimdienste nicht binden kann. Die kommende Datenschutz-Grundverordnung der EU wird mit ihrem Marktortprinzip zudem hoffentlich dafür sorgen, dass der Datenabfluss bei amerikanischen Anbietern transparenter wird.“

Der nationale Datenschutz sei in der Spähaffäre weitgehend hilflos, räumte der Landesbeauftragte ein: „Es ist schon frustrierend, wenn wir uns permanent um alltägliche Datenschutzprobleme kümmern – um die unerwünschte Werbe-E-Mail ebenso wie um den Nachbarstreit wegen einer Videokamera, um im Polizeicomputer gespeicherte „Jugendsünden“ ebenso wie um überquellende Behördenbriefkästen – und wenn das Bundesverfassungsgericht das Verbot einer Totalüberwachung zur verfassungsrechtlichen Identität unseres Landes rechnet, und auf der anderen Seite greifen ausländische Nachrichtendienste ungeniert auf den gesamten weltweiten Kommunikations- und Internetverkehr zu. Die Privatsphäre wird auf diese Weise ad absurdum geführt.“ Immerhin habe aber die NSA-Affäre wie ein Weckruf gewirkt und – wie Umfragen zeigten – das Bewusstsein für die Datensicherheit bei Privatleuten und in der Wirtschaft deutlich wachsen lassen. „Das Vertrauen in Angebote mit amerikanischer Beteiligung, z.B. bei Cloud Computing, hat massiv gelitten“, ergänzte Jörg Klingbeil, „gerade bei den mittelständischen Unternehmen in Baden-Württemberg ist eine erhebliche Verunsicherung zu spüren. Dieser Vertrauensverlust ist jetzt eine Chance für Datenschutz made in Europe“. Ob es sinnvolle nationale Lösungen für das Internet geben könne, sei dagegen eher zweifelhaft: „Wir können die Entwicklung nicht zurückdrehen, aber vielleicht doch mehr Kontrolle zurückerlangen, z. B. durch ein Routing innerhalb Europas. Wichtig wäre auch, dass wir mehr Einfluss auf die internationalen Standardisierungsverfahren gewinnen, denn da mischt die NSA kräftig mit.“ Im Übrigen sei es zu einseitig, jetzt nur eine Bedrohung durch US-amerikanische und britische Dienste an die Wand zu malen, denn russische und chinesische Dienste würden sich im Internet genauso tummeln und kriminelle sowieso. Insofern seien Datenschutz und Datensicherheit unabhängig von der NSA-Affäre das Gebot der Stunde.

Die unter dem Schlagwort „Big Data“ propagierte Sammlung und Auswertung großer Datenmengen macht nach den Worten des Datenschutzbeauftragten deutlich, dass Daten zunehmend zum Rohstoff des 21. Jahrhunderts werden, an dem viele partizipieren wollen: „Das Thema ist mehr als ein aktueller ‚Hype‘. Im Grunde wird hier die gleiche Methode wie bei den Geheimdiensten angewandt: Datenberge werden angelegt und nach Mustern durchsucht, die Computer lernen dazu und sollen am Ende komplexe Prozesse selbsttätig steuern.“

Nach Einschätzung des Landesbeauftragten wird dem Geschäftsmodell Big Data aber nur dann dauerhafter Erfolg beschieden sein, wenn die erhobenen personenbezogenen Daten wirksam anonymisiert werden und keine Rückschlüsse auf Personen

mehr möglich sind. Andernfalls drohten Missbrauch und Kontrollverlust. Der Datenschutz müsse von Anfang an eingebaut werden (sog. *privacy by design*); hierfür sei noch viel konzeptionelle Arbeit zu leisten.

Ein künftiger Anwendungsbereich für Big Data wird nach Ansicht des Landesdatenschutzbeauftragten der Verkehr sein: „Die Industrie rüstet bereits kräftig auf. Ab dem nächsten Jahr soll der von der EU vorgegebene automatische Notruf (e-Call) in den Fahrzeugen Einzug halten. Damit wird ein Einfallstor für weitere Telematikanwendungen geschaffen; hierfür gibt es schon zahlreiche Ideen. Die intelligenten Autos sollen untereinander, mit den Herstellerfirmen, den Werkstätten, anderen Dienstleistern und der Straßeninfrastruktur, auch über das Internet, vernetzt werden. Ohne personenbeziehbare Daten wird das kaum gehen; damit droht uns bald der gläserne Autofahrer. Von tauglichen Datenschutzkonzepten und einer tragfähigen Rechtsgrundlage ist aber weit und breit noch nichts zu sehen! Diese muss nun alsbald geschaffen werden, sonst gerät der Datenschutz im wahrsten Sinne des Wortes unter die Räder.“ Jörg Klingbeil kündigte an, dass sich seine Dienststelle auch in Zukunft mit diesem für Baden-Württemberg wichtigen Thema verstärkt befassen werde.

Hier steht der Bericht zur Verfügung: <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/01/31.-TB-2012-2013.pdf#>

## LfDI NRW: Mehr Transparenz bei den Scorewerten von Auskunfteien schaffen

Der Bundesgerichtshof hat am 28.01.2014 über den Umfang einer von der SCHUFA zu erteilenden Auskunft zum sogenannten Scorewert entschieden, also zu einem mathematisch erstellten Prognosewert zur Zahlungsfähigkeit. Danach haben die Kunden keinen Anspruch darauf, von der SCHUFA zu erfahren, wie die zu ihrer Person in den Scorewert eingeflossenen Einzelmerkmale von der Auskunftei gewichtet und auch nicht welche Vergleichsgruppen herangezogen worden sind.

Ulrich Lepper hierzu: „Die für die Verbraucher notwendige Transparenz zu ihren Bonitätswerten bleibt auf halber Strecke stehen. Ich fordere die neue Bundesregierung auf, die gesetzliche Regelung im Bundesdatenschutzgesetz zur Auskunft über das Scoringverfahren datenschutzfreundlicher zu gestalten. Dazu gehört Klarheit über die verwendeten Verfahren. Es dürfen zudem nur Daten verwendet werden, die für die Zahlungsfähigkeit von Bedeutung sind. Da die Arbeiten zur Evaluierung der Bundesdatenschutz-Novelle aus dem Jahr 2009 derzeit laufen, bietet sich hierzu auch eine gute Chance.“

Der Bundesgerichtshof hatte in seiner gestrigen Entscheidung (Urteil vom 28. Januar 2014 – VI ZR 156/13) aber auch deutlich gemacht, dass der Auskunftsanspruch nach § 34 Bundesdatenschutzgesetz die Auskunfteien schon jetzt verpflichtet, den Verbrauchern Auskunft darüber zu erteilen, welche personenbezogenen – insbesondere kreditrelevanten – Daten bei ihnen gespeichert und in die Berechnung des Scorewerts eingeflossen sind. Zudem sind die Verbraucher darüber zu informieren, welche Wahrscheinlichkeitswerte in den letzten zwölf Monaten an Dritte übermittelt wurden, wie der aktuell berechnete Scorewert lautet und welche Daten zur Berechnung genutzt wurden.