RFID und datenschutzrechtliche Transparenz

Der Beitrag erwidert in einem Punkt auf *Holznagel/Bonnekoh*, MMR 2006, 17. Er nimmt dies zum Anlass, auf eine grundsätzliche Schwierigkeit der rechtlichen Bewertung neuer Technologien hinzuweisen, erörtert die problematische Anwendung von § 6c BDSG auf RFID-Tags und weist auf die Notwendigkeit der Beachtung des Transparenzprinzips hin.

1. Problemstellung

Die Anwendung gesetzlicher Regelungen auf neue technische Entwicklungen bereitet mitunter erhebliche Probleme. Hintergrund kann das Bemühen des Gesetzgebers sein, mit einer Norm nicht nur die zum Zeitpunkt des Erlasses bereits bekannten Technologien zu erfassen, sondern auch künftige, deren Entwicklung entweder nur vermutet wird oder sogar gänzlich unbekannt ist. So definiert z.B. § 2 Abs. 1 TDG Teledienste als „alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zu Grunde liegt". Bei dieser Definition hat deutlich eine Reihe von Anwendungen des Internet Pate gestanden, die auch in § 2 Abs. 2 TDG beispielhaft genannt sind (zur Abgrenzung zu Mediendiensten s. *Spindler*, in: Roßnagel, Recht der Multimediadienste, § 2 TDG Rdnr. 13 ff.; *Meier*, ebd., § 2 MDStV Rdnr. 20 ff.). Derartige abstrakte Beschreibungen sind in ihrem Streben nach zukunftsgerichteter Regelung grds. begrüßenswert. Sie bergen aber auch die Gefahr, nur einen Ausschnitt einer neuen Technologie zu erfassen und einen anderen – naturgemäß unbeabsichtigt, dennoch i.E. mehr oder weniger willkürlich – auszunehmen.

2. Die Reichweite von § 6c BDSG

a) Was sind „mobile personenbezogene Speicher- und Verarbeitungsmedien"?

Ein weiteres Beispiel der erwähnten Regelungstechnik sind „mobile personenbezogene Speicher- und Verarbeitungsmedien", für die § 6c BDSG besondere Transparenzregeln aufstellt (zu Anwendungsbereich und Reichweite von § 6c BDSG s. z.B. *Bizer*, in: Simitis, BDSG, 5. Aufl. 2003, § 6c Rdnr. 2 ff.; *Gola/Schomerus*, BDSG, 8. Aufl. 2005, § 6c Rdnr. 1 ff.; *Hornung*, DuD 2004, 15 ff.; ausf. *ders.*, Die digitale Identität, 2005, S. 253 ff.). Diese Medien sollen ausweislich der Definition in § 3 Abs. 10 BDSG verstanden werden als „Datenträger, 1. die an den Betroffenen ausgegeben werden, 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.". Ganz offensichtlich dachte der Gesetzgeber an dieser Stelle an die Chipkarte in ihrer Ausprägung als Mikroprozessorkarte (zu den datenschutzrechtlichen Problemen von Chipkarten s. z.B. *Weichert*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 9.5; *Bizer*, in: v. Zezschwitz/Möller, Verwaltung im Zeitalter des Internet, 2002, S. 19 ff.; *Hornung*, Die digitale Identität, 2005). Die Gesetzesbegründung betont aber, es komme nicht auf die Gestaltung des Mediums an (BT-Drs. 14/5793, S. 60).

Nimmt man die Definition in § 3 Abs. 10 Nr. 2 BDSG ernst, so fällt auf, dass sie eine erhebliche Einschränkung darstellt. Anders als etwa in § 32 Abs. 1 des Entwurfs von *Bündnis 90/DIE GRÜNEN* aus dem Jahr 1997 (BT-Drs. 13/9082, S. 12) und in einigen Landesdatenschutzgesetzen (z.B. § 5b HmbDSG, § 3 Abs. 10 DSG MV; mehrdeutig § 5 Abs. 3 BbgDSG; s. zu den landesrechtlichen Regelungen näher *Hornung*, DuD 2004, 15, 17 f.; *ders.*, Die digitale Identität, 2005, 261 ff.) reicht die direkte Kommunikation mit elektronischen Lese- und Schreibgeräten nicht aus. Vielmehr muss auf dem Medium selbst eine „automatisierte Verarbeitung" stattfinden. Dieser Begriff umfasst nach § 3 Abs. 2 BDSG – sprachlich missglückt (s. *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 31 f.; *Dammann*, in: Simitis, BDSG, § 3 Rdnr. 64) – den engeren Tatbestand des Verarbeitens nach § 3 Abs. 4 BDSG, darüber hinaus aber auch die Erhebung und Nutzung personenbezogener Daten, allerdings immer unter der Voraussetzung des Einsatzes von DV-Anlagen.

Damit wird eine der derzeit am häufigsten ausgegebenen Karten nicht erfasst, nämlich die Kundenkarte: „Auf" dieser werden – zumindest bei den bisherigen technischen Ausprägungen – regelmäßig gerade keine Daten verarbeitet. Das ist für die Sichtkarte oder Karten mit einem opto-elektronisch auslesbaren Barcode evident, gilt aber auch für Chipkarten, solange diese lediglich die Stammdaten des Kunden speichern und

zum Auslesen an der Kasse bereitstellen. Gerade weil hier kein wesentlicher Unterschied zum Barcode oder zur Magnetkarte besteht, fallen diese „dummen" Karten nicht unter § 3 Abs. 10 BDSG und damit auch nicht unter die Transparenzvorschrift des § 6c BDSG (das bedeutet natürlich nicht, dass Kundenkarten auch in einfachen Ausprägungen keine datenschutzrechtlichen Probleme hervorrufen würden; s. dazu etwa *ULD Schleswig-Holstein*, Kundenbindungssysteme und Datenschutz, 2003; *Weichert*, DuD 2003, 161 ff.; *Körffer*, DuD 2004, 267 ff.). Dieser Gedanke wird auch in der Gesetzesbegründung betont (BT-Drs. 14/5793, S. 60, 63 f.).

b) RFID-Chips

Die Einschränkung in § 3 Abs. 10 Nr. 2 BDSG findet nicht immer Beachtung im Schrifttum. So wird vertreten, es komme weder auf die Beschaffenheit des Datenträgers noch darauf an, ob sich auf ihm ein Mikrochip befinde (*Weichert*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 9.5, Rdnr. 20). Einige Autoren betonen zwar zutreffend, Medien, die lediglich ein automatisiertes Auslesen von Informationen ermöglichten, erfüllten nicht die Voraussetzungen von § 3 Abs. 10 BDSG, sind jedoch zugleich der pauschalen Ansicht, Kundenkarten seien von der Vorschrift gerade erfasst (*Holznagel/Bonnekoh*, MMR 2006, 17, 21; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 311; *Eisenberg/Puschke/Singelnstein*, ZRP 2005, 9 (s. dort Fußn. 5); *Gräfin von Westerholt/Döring*, CR 2004, 710, 714; letztere unter Verweis auf *Bizer*, in: Simitis, BDSG, § 6c Rdnr. 6 f. Die zitierte Stelle ist insoweit missverständlich, als i.R.d. Erläuterungen zum Anwendungsbereich von § 6c BDSG ein Überblick über Chipkartensysteme gegeben wird, die nicht alle unter die Norm fallen; eindeutig demgegenüber *Bizer*, ebd., § 3 Rdnr. 277). Dass sich diese Aussagen zumindest z.T. widersprechen (s.o.), wird nicht erkannt.

In der Folge findet sich in der datenschutzrechtlichen Diskussion um RFID-Systeme (s. außer den Beiträgen unten in diesem Absatz z.B. *FoeBuD e.V. et al.*, Positionspapier über den Gebrauch von RFID, http://www.foebud.org/texte/aktion/rfid/positionspapier.pdf, 2003; *Müller*, DuD 2004, 215 ff.; *ders./Handy*, DuD 2004, 655 ff.; *Hansen/Wiese*, DuD 2004, 109 ff.; *Conrad*, CR 2005, 537 ff.; zur strafprozessualen Perspektive vgl. *Eisenberg/Puschke/Singelnstein*, ZRP 2005, 10 ff.; aus technischer Sicht s. *Kelter/Wittmann*, DuD 2004, 331 ff.; *BSI*, Risiken und Chancen des Einsatzes von RFID-Systemen, 2004) – zuletzt im Beitrag von *Holznagel/Bonnekoh* – die Ansicht, der Anwendungsbereich von § 6c BDSG sei betroffen, wenn „eine Kundenkarte mit einem RFID-Chip ausgestattet [ist], auf dem personenbezogene Daten gespeichert sind" (*Holznagel/Bonnekoh*, MMR 2006, 17, 21; ebenso *v. Westerholt/Döring*, CR 2004, 710, 714). Diese Aussage steht nicht nur in direktem Widerspruch zu § 3 Abs. 10 Nr. 2 BDSG, der gerade eine automatisierte Verarbeitung dieser Daten „über die Speicherung hinaus" verlangt. Wie erläutert, entspricht diese Beschränkung auch dem gesetzgeberischen Willen und dem Zweck der Vorschrift.

Das bedeutet umgekehrt zwar nicht, dass Kundenkarten niemals mobile personenbezogene Speicher- und Verarbeitungsmedien sein können. Ob dies der Fall ist, richtet sich aber nicht danach, ob die Datenübertragung mittels eines RFID-Systems erfolgt. Um es genauer auszudrücken: Der Anwendungsbereich von § 3 Abs. 10 BDSG ist gar kein Problem der RFID-Technologie, wenn und soweit mit diesem Begriff eine Schnittstellentechnologie (nämlich die Datenübertragung mit Radiofrequenzwellen) bezeichnet wird. Die Definition setzt nicht an der Schnittstelle, sondern an der Datenverarbeitung „dahinter", also auf dem Medium an. Je nach Art der Verarbeitungsprozesse wird dieses Medium also tatsächlich von §§ 3 Abs. 10 Nr. 2 und 6c BDSG erfasst – die drahtlose Datenübertragung ist hierfür aber kein Abgrenzungskriterium.

3. Transparenz als datenschutzrechtliche Grundanforderung – auch bei RFID

Hinter § 6c BDSG steht der Gedanke, dass wegen der Intransparenz einer Verarbeitung auf mobilen personenbezogenen Speicher- und Verarbeitungsmedien erhöhte datenschutzrechtliche Gefahren für den Betroffenen entstehen, denen durch die Festlegung von Informationspflichten begegnet werden soll (s. die Gesetzesbegründung, BT-Drs. 14/5793, S. 63; *Bizer*, in: Simitis, BDSG, § 6c Rdnr. 3; *Gola/Schomerus*, BDSG, § 6c Rdnr. 2). Das Problem der Intransparenz stellt sich auch bei RFID-Systemen, soweit diese personenbezogene Daten verwenden. Es wird hier aber im Kern nicht durch die Intransparenz der Datenverarbeitung auf dem Chip, sondern durch die Intransparenz der Datenübermittlung zwischen Tag und Lesegerät ausgelöst. Auch bei einfachsten, passiven Tags, die nur eine – personenbeziehbare – Nummer speichern, kann durch die unmerkliche Einbindung in ein größeres DV-System ein datenschutzrechtliches Problempotenzial entstehen.

An dieser Stelle zeigt sich die Schwäche (oder immanente Grenze) der eingangs erläuterten Regelungstechnik. Da der Gesetzgeber bei der Konzeption von § 6c BDSG ganz offensichtlich die bisherigen Ausprägungen der Chipkarte im Blick hatte (die datenschutzrechtlichen Probleme von RFID-Chips waren noch nicht bekannt), ist die Norm nur auf eine Teilgruppe dieser Chips anwendbar, deren Abgrenzung zweifelhaft ist. Vertreten wird, im Rahmen von § 6c BDSG müsse die automatisierte Verarbeitung lediglich teilweise auf dem RFID-Tag ablaufen (*Lahner*, DuD 2004, 723, 725). Das ist nicht zutreffend, weil die Norm in allen Varianten ein Medium i.S.v. § 3 Abs. 10 BDSG voraussetzt, der diese Einschränkung nicht enthält. Auch die Aussage, die automatisierte Datenübermittlung zwischen Tag und Leser reiche bereits für das Merkmal des „automatisierten Verarbeitens über die Speicherung hinaus" aus (ebd., 725 f.), überzeugt nicht, weil dann auch reine Speichermedien erfasst wären. Das widerspricht dem klaren Willen des Gesetzgebers (*Hornung*, DuD 2004, 15, 16; *ders.*, Die digitale Identität, 2005, 258 f.).

Die Anwendbarkeit von § 6c BDSG – und anderer datenschutzrechtlicher Normen – auf RFID-Systeme muss de lege lata zwar beantwortet werden. Wenn RFID-Systeme allerdings wesentlich durch die Unmerklichkeit der Datenübermittlung mit dem Transparenzprinzip in Konflikt geraten, so ist es nicht an-

gemessen, datenschutzrechtliche Aufklärungspflichten an die Frage zu knüpfen, ob auf den Tags selbst i.S.v. § 3 Abs. 10 Nr. 2 BDSG Daten automatisiert verarbeitet werden können. Das Transparenzprinzip ist eine verfassungsrechtlich begründete Ausprägung des Rechts auf informationelle Selbstbestimmung (*Gola/Schomerus*, BDSG, § 33 Rdnr. 1; *Podlech*, in: Denninger/Hoffmann-Riem/Schneider/Stein, Alternativkommentar zum GG, Art. 2 Abs. 1 Rdnr. 81; das *BVerfG* hat formuliert, mit dem Recht auf informationelle Selbstbestimmung sei eine Gesellschafts- und Rechtsordnung nicht vereinbar, „in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß", BVerfGE 65, 1, 43). Seine Anwendung auf eine neue Technologie wie RFID-Systeme kann man im Einzelfall je nach technischer Ausprägung durch Spezialregelungen wie § 6c BDSG begründen – das ändert aber nichts daran, dass es für jede Form der Datenverwendung gilt.

Ob dem Transparenzgrundsatz in Bezug auf die RFID-Technologie im geltenden Datenschutzrecht hinreichend genügt wird, muss – ohne dies hier ausführlich zu erörtern – als durchaus fraglich bezeichnet werden (s. zum Problem der Transparenz *FoeBuD e.V. et al.*, Positionspapier über den Gebrauch von RFID, http://www.foebud.org/texte/aktion/rfid/positionspapier.pdf, 2003, S. 4; *Müller/Handy*, DuD 2004, 657; *Conrad*, CR 2005, 537, 539; allg. für das Ubiquitous Computing *Roßnagel/Müller*, CR 2004, 625, 628 f.; zur Transparenz bei Chipkarten auch *Weichert*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 9.5 Rdnr. 47 ff.). Nicht hinreichend ist es jedenfalls, aus der Tatsache, dass das geltende Datenschutzrecht „sämtliche Varianten der Transpondertechnologie erfasst", zu folgern, es seien „keine Gesetzeslücken ersichtlich" (*Holznagel/Bonnekoh*, MMR 2006, 17, 23). Dass das Datenschutzrecht eine neue Technologie erfasst, bedeutet noch nicht, dass es die neuen Konfliktlagen auch sachgerecht löst. So führt die Anwendung der allgemeinen Regeln über die Datenverarbeitung nicht öffentlicher Stellen eben auch dazu, dass ein Einsatz von RFID-Tags zur Durchführung von Werbemaßnahmen und Marktanalysen – ohne Einwilligung der Betroffenen – jedenfalls hinsichtlich der Stammdaten der Kunden gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG für zulässig gehalten wird (*Holznagel/Bonnekoh*, MMR 2006, 17, 20).

Grundsätzlicher zeichnet sich ab, dass die Anwendung der bisherigen datenschutzrechtlichen Regeln über Transparenz, Einwilligung, Zweckbindung und Betroffenenrechte in einer Welt des Ubiquitous Computing – für die RFID-Systeme ein potenzieller Baustein sind – vielfach weder praktikabel noch sachgerecht sein wird (*Roßnagel/Müller*, CR 2004, 625, 628 ff.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, S. 185 f.). Die bevorstehende umfassende Einführung von RFID-Systemen sollte ein willkommener Anlass sein, die anstehende Modernisierung des Datenschutzrechts anhand eines praktischen Beispiels zu diskutieren.

Dr. Gerrit Hornung, LL.M., Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel.