Ulrich Eisenberg, Jens Puschke, Tobias Singelnstein

Ubiquitäres Computing = ubiquitäre Kontrolle?

Zum Potential der RFID-Technologie für Überwachung und Kontrolle

Analysen sicherheitspolitischer Konzepte gehen davon aus, dass Strategien sozialer Kontrolle zunehmend ergänzt werden durch neuartige Techniken, vor allem in Form von (technischen) Kontrollarrangements, die sehr frühzeitig und eher subtil auf Geschehensabläufe einwirken. Gleichzeitig werden die herkömmlichen Formen strafprozessualer wie auch präventivpolizeilicher Überwachung[1] ständig ausgeweitet: Gerade die Verbreitung von Computern und der Gebrauch des Mobilfunks haben gezeigt, dass vorbehaltlich bestimmter strafprozessualer Verbote nahezu alles, was technisch möglich ist bzw. gespeichert vorliegt, auch eingesetzt bzw. ausgewertet wird. Beide Entwicklungen sind eng verbunden mit dem technischen Fortschritt, und hier insbesondere mit zwei Aspekten. Zum einen erlauben neue technische Möglichkeiten immer weitere, effektivere und einfachere Formen der Kontrolle und Überwachung;[2] zum anderen steigt die Art und der Umfang gespeicherter Daten in allen Lebensbereichen weiter an, so dass die Aufgabe der Informationsbeschaffung aus diesem Pool zunehmend eine Frage vor allem der technischen Möglichkeiten des Auswertens und der Auswahl und im Rahmen dessen auch der Herstellung eines Personenbezuges wird.

Sowohl der Aspekt der Informationsbeschaffung als auch derjenige neuer Formen und Möglichkeiten der Ausforschung finden sich wieder in der Entwicklung des ubiquitären Computings. Hierunter wird eine neue Generation allgegenwärtiger Datenverarbeitung verstanden, die heute noch kaum

1 Unter Überwachung werden im Folgenden die vor allem in den Polizeigesetzen und der StPO geregelten Maßnahmen zur regelmäßig personenbezogenen Informationserlangung für repressive und präventive Zwecke verstanden. Demgegenüber werden unter den Begriff der neueren technischen Kontrolltechniken Arrangements gefasst, die eher situativ alle dort betroffenen Personen erfassen, weit im Vorfeld eingreifen und – mitunter manipulativ – Verhalten beeinflussen (z.B. Zugangsbeschränkungen, Videoüberwachung u. Ä.).

2 Zu denken ist bspw. nur an das GPS-System, den Mobilfunk sowie die damit verbundenen Möglichkeiten der Standortbestimmung und den in Einführung befindlichen automatischen Kfz-Kennzeichenabgleich.

vorstellbare Möglichkeiten eröffnet und damit Datenschutz und sonstige rechtliche Begrenzungen mit veränderten Herausforderungen konfrontiert.[3] Besonders deutlich wird dies derzeit angesichts der Technik der Radio Frequency Identification (RFID, Funkidentifikation, auch *smart labels* genannt). Dabei handelt sich um einen mit bloßem Auge kaum wahrnehmbaren Speicherchip, dessen Daten aus der Distanz und unbemerkt abgefragt werden können, der vielseitig einsetzbar ist und voraussichtlich in naher Zukunft in zahlreichen Lebensbereichen präsent sein wird. Seine Nützlichkeit für Abläufe nicht nur in der Wirtschaft ist unbestritten, während vor allem hinsichtlich des Datenschutzes eine lebhafte Debatte um das Gefahrenpotential dieser Technik geführt wird (BT-Drs. 15/3025; BSI 2004: 100ff.; Gräfin von Westerholt/Döring 2004: 710ff.).

Der folgende Beitrag untersucht aus kriminologischer Sicht das Potential von RFID im Hinblick auf Kontrolle und Überwachung. Hierfür wird zunächst eine technische und rechtliche Einführung gegeben, um sodann mögliche Funktionen und Einsatzbereiche zu erörtern und sich deren kriminologischen Aspekten zu widmen.

I. Technische und rechtliche Einführung

1. Technischer Hintergrund

Bei RFID handelt es sich um eine *Technik zur Identifizierung* basierend auf (automatischer) Datenübermittlung mittels Funksignalen. Hierfür werden auf winzig kleinen Transponderchips gespeicherte Daten von einem als Empfangseinheit fungierenden Lese- und Schreibgerät ausgelesen,[4] ohne dass dabei eine Sicht- oder sonstige direkte Verbindung erforderlich wäre. Die Technik ermöglicht somit das Auslesen und Verändern der gespeicherten Daten unabhängig von Sichtbarrieren wie Wänden, Taschen, Kleidungsstücken und auch *unabhängig* von der *Kenntnisnahme des Betroffenen*, so dass der Frage der Verschlüsselung der gespeicherten Daten wie auch der Deaktivierung der Chips nach Funktionserfüllung eine erhebliche Relevanz zukommt. Abhängig von der konkreten technischen Ausgestaltung können die Daten aus einer Entfernung von einigen Zentimetern bis zu

3 Im Auftrag des Bundesministeriums für Bildung und Forschung erstellt das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) daher derzeit eine Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS).

4 Die Geräte sind fast so flach wie Papier und zum Teil nur wenige Quadratmillimeter groß. Indes wirkt sich die Größe auch auf Speicherkapazität und Reichweite aus. In einer passiven Transpondereinheit (ohne eigene Stromversorgung) wird durch die Absendung eines Funksignals vom Lese-/Schreibgerät ein magnetisches Feld erzeugt, welches die Sendung der Daten auslöst. Ein aktiver Transponder mit größerer Speicherkapazität kann mittels eigener Stromversorgung weitergehende Funktionen, wie die Verschlüsselung der Daten, durchführen.

etwa 30 Metern (vgl. Hansen/Wiese 2004: 109) und mit hohem Tempo ausgelesen werden: Die Lesegeräte sind auch noch bei hoher Passiergeschwindigkeit in der Lage, bis zu 200 Chips pro Sekunde zu erfassen.

Die Verbreitung der Technologie – vor allem im wirtschaftlichen Bereich – wird erheblich von den Stückkosten für die einzelne Transpondereinheit abhängig sein. Schätzungen zufolge ist über den Ablauf weniger Jahre hinweg von einer deutlichen Absenkung der Kosten auszugehen. Dabei werden die Einsparpotentiale durch Rationalisierung für den deutschen Einzelhandel mit ca. 6 Mrd. Euro pro Jahr beziffert (vgl. hierzu BSI 2004: 66), so dass eine eher hohe Investitionsbereitschaft für die Weiterentwicklung von RFID-Systemen zu erwarten ist.

2. Verfassungsrechtliche Grundlagen

Rechtlich ist der Einsatz von RFID-Chips ausgehend von den Grundrechten zu bewerten. Tangiert ist hier insbesondere das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in der Ausformung des *Grundrechts* auf *informationelle Selbstbestimmung*, das die Befugnis des Einzelnen zur eigenen Entscheidung über die Offenbarung persönlicher Lebenssachverhalte beinhaltet (BVerfGE 65: 41ff.; Dreier 2004: Art. 2 Abs. 1, Rn. 78). Der staatliche Einsatz der RFID-Technologie zum Zweck der Kontrolle und Überwachung stellt bei der Nutzung auf dem Chip gespeicherter personenbezogener bzw. personenbeziehbarer Daten einen Eingriff in das Grundrecht dar und erfordert somit das Vorliegen einer Ermächtigungsgrundlage. Beim Einsatz durch Private gelten entsprechend die Regelungen über die mittelbare Drittwirkung von Grundrechten (vgl. von Münch 2000: Vorb. Art. 1-19, Rn. 28ff.).

Derartige Ermächtigungen wie auch die Abwägung im Rahmen der Drittwirkung haben insbesondere auch der speziellen Qualität einer Überwachung mittels RFID Rechnung zur tragen. So ergeben sich erhöhte Anforderungen aus dem Bestimmtheitsgebot und dem Verhältnismäßigkeitsgrundsatz; dabei ist eine Totalausforschung bzw. Persönlichkeitsprofilerstellung in jedem Fall unzulässig (vgl. BVerfGE 27: 6; 65: 53; BVerfG NJW 2004: 1004; Puschke 2005). Zur Vermeidung derartiger Grundrechtsverletzungen sind entsprechende gesetzliche Regelungen erforderlich, wobei zu berücksichtigen ist, dass das Grundrecht auf informationelle Selbstbestimmung gerade im Hinblick auf die Allgegenwart und dauernde Verwendung personenbezogener Daten und die Entwicklung entsprechender Technik geschaffen wurde (BVerfGE 65: 42).

3. Eingriffsgrundlagen und Regelungsbedarf

Während also bei einer Verwendung von RFID durch Private die Grundrechte jeweils im Rahmen der einzelfallbezogenen Abwägung zu berücksichtigen sind, ist für staatliche Stellen eine Eingriffsgrundlage erforderlich.

Eine Betrachtung bereits bestehender Ermächtigungen alleine im Bereich der Strafverfolgung lässt einerseits erkennen, dass gewisse Formen des Einsatzes von RFID schon heute durch diese Regelungen erfasst sind (Eisenberg/Puschke/Singelnstein 2005: 10f.). Im Einzelnen scheinen bspw. die Regelungen über die Beschlagnahme (§§ 94 ff. StPO),[5] den Einsatz technischer Mittel (§ 100c Abs. 1 Nr. 1 b StPO) zur Sachverhaltserforschung oder Aufenthaltsermittlung (vgl. Eisenberg 2002: Rn. 2427ff.; Meyer-Goßner 2004: § 100c, Rn. 2f.) oder ggf. sogar solche über Kontrollstellen (§ 111 StPO) bestimmte Formen der Nutzung von RFID bzw. der darauf gespeicherten Daten zuzulassen. Darüber hinaus steht zu erwarten, dass mit zunehmender Verbreitung der Technik weitergehende Rechtsgrundlagen geschaffen werden.

Zum anderen wird hieran deutlich, dass das bestehende System strafprozessualer Eingriffsgrundlagen im Hinblick auf den Einsatz ubiquitären Computings den verfassungsrechtlichen Vorgaben und Grenzen nicht (mehr) in vollem Maße gerecht werden kann[6] – unabhängig davon, ob man diese nun im Grundsatz der Verhältnismäßigkeit, dem Wesensgehalt der Grundrechte oder dem aus Art. 1 Abs. 1 GG folgenden absolut geschützten Kernbereich persönlicher Lebensgestaltung sieht (BVerfG NJW 2004: 999ff.; BGH NStZ 1999: 147; Eisenberg/Puschke/Singelnstein 2005; Wolter 2004: 745ff.). Dies legt eine Neugestaltung des Regimes der einschlägigen Eingriffsbefugnisse nicht nur nahe, sondern macht sie auch erforderlich. Dabei ist es notwendig, eine Kumulation verschiedener Überwachungsmethoden unter besondere Voraussetzungen zu stellen, da ansonsten auf diesem Wege eine umfassende Ausforschung möglich würde (näher Puschke 2005; Wolter 2004: 746). Dies entspricht auch einer notwendigen Anpassung an eine Entwicklung dahingehend, dass Menschen zunehmend bei nahezu jeder Tätigkeit Datenspuren hinterlassen, was gerade durch einen umfassenden Einsatz der RFID-Technologie in besonderem Maße verstärkt wird. De lege ferenda sollte daher solche Informationsbeschaffung nach dem jeweiligen Zweck differenzierend und speziell geregelt und dabei besonderen Voraussetzungen unterstellt werden, die das umfassende Ausmaß damit ermöglichter Ausforschung berücksichtigen (vgl. auch Demko 2004: 63f.).

---

5 Vgl. zur Auswertung beschlagnahmter Datenträger bspw. BVerfG NStZ-RR 2003: 177; Nack 2003: § 94, Rn. 4; § 98a, Rn. 4 f.; zum Abruf der Daten aus einer Mobilbox nach Beschlagnahme vgl. Bär 2000: 476.

6 Insbesondere bezieht sich RFID nicht auf einzelne, abgrenzbare Lebensbereiche, sondern bietet die Möglichkeit einfacher Informationsgewinnung – bei einer mittelbaren Nutzung auch ohne vorheriges Handeln durch staatliche Organe – auf nahezu allen Ebenen des Privatlebens. Spätestens mit dieser Möglichkeit der Erstellung von Persönlichkeitsbildern sind die verfassungsrechtlichen Grenzen für Überwachung überschritten.

II. Funktion und Einsatzbereiche der RFID-Technologie

Die Nutzung der RFID-Technologie kommt für Formen klassischer disziplinierender Überwachung wie auch neuere Kontrolltechniken in Betracht. Während Erstere regelmäßig personenbezogen und anlassabhängig auf die Informationsgewinnung gerichtet sind, wird bei technischen Kontrollarrangements eher situationsgebunden und bezüglich aller dann Betroffenen ein Istwert mit einem Sollwert verglichen, woraus sich die mögliche Folge des Auslösens einer Konsequenz ergibt. Gerade diese Kontrolltechniken werden in erheblichem Umfang (auch) im wirtschaftlichen Bereich und von Privaten eingesetzt. Obwohl sie sehr viel früher und im Vorfeld eingreifen, überschneiden sie sich mit Überwachungsformen, und beide Bereiche nähern sich an.

1. Allgemeine Funktionen und Merkmale

Allgemein gefasst und auf den Kern zurückgeführt dient die RFID-Technik zunächst einmal (nur) der Bezeichnung und daraus folgend der Möglichkeit der Identifizierung von Sachen oder Personen. Hieraus ergeben sich indes zahlreiche andere Funktionen, die bei einer Verbindung mit weiterer Technik bzw. von verschiedenen Formen von Daten oder Funktionen möglich werden, wie z.B. Ortung, Erlangung von Informationen etc. Dabei lässt sich differenzieren zwischen einerseits Funktionen, die sich unmittelbar aus der Technik ergeben, d.h. aus dem Umstand, dass ein Objekt mit einem Chip und darauf gespeicherten Daten verbunden ist. Andererseits sind Techniken erkennbar, die sich (nur) auf den entstehenden Datenpool hinter den Lesegeräten wie auch auf den Chips stützen, wobei auch hier die Möglichkeit der Personenbeziehbarkeit von Relevanz ist – sofern nicht die auf dem Chip gespeicherten Daten wie bei Ausweisen ohnehin personenbezogen sind.

Diese Differenzierung entspricht der eingangs vorgenommenen Unterscheidung zwischen dem Aspekt der Informationsbeschaffung aus Datenmassen und demjenigen neuer Formen und Möglichkeiten der Kontrolle. Sie spiegelt damit das Innovationspotential der RFID-Technik für Staat wie auch Private wider: Einerseits werden immer mehr Daten in immer mehr Lebensbereichen produziert, gespeichert und so für eine Informationsgewinnung nutzbar gemacht; zum anderen ermöglicht die Technik nicht nur eine Vereinfachung von Kontrollverfahren sondern auch ganz neue Formen, in dem sie bspw. verschiedene Varianten der Kontrolle verbindet. Dabei zeigen sich jeweils neben der Identifizierung weitere mögliche Funktionen, wie die Positionsbestimmung, daten- und ereignisbezogene Detektion – i.S.d. Feststellung von Abweichung – und die Informationserlangung i.e.S.[7]

7 So die von Nogala (2001) entwickelte Systematisierung verschiedener Funktionen von Kontrolle und Überwachung, wobei die vorgeschlagene Differenzierung in sol-

2. *Funktionen und Einsatzbereiche unmittelbar durch die Verbindung von Chip und Objekt*

Die RFID-Technologie wurde im und für den wirtschaftlichen Bereich entwickelt, wo sie vor allem den so genannten Barcode zur Übermittlung einer Produktkennung auf der Grundlage einer optischen Scanvorrichtung ersetzen soll. Entsprechend liegt der aktuelle Schwerpunkt der Entwicklung und Verwendung auf der Produkterkennung im Einzelhandel bzw. auf der Lagerverwaltung und Bestandsadministration von Unternehmen.[8] Mittelfristiges Ziel ist die Bestückung aller Produkte mit RFID-Chips zur weltweit eindeutigen Identifizierung.[9] Dies dient vor allem einer lückenlosen Nachvollziehbarkeit der einzelnen Prozesse der Produktherstellung bzw. des Transports und Verkaufs. Diese *Funktion der Identifizierung* ist auch betroffen, soweit es um den Einsatzbereich der automatisierten Zutrittsbegrenzung[10], Diebstahlssicherungen z.B. in Form von Wegfahrsperren oder auch der Verwendung in Pässen in Verbindung mit Biometrie geht.

Aus dieser ursprünglichen Funktion der Identifizierung lassen sich durch eine Kombination mit sonstiger Technik weitere Möglichkeiten entwickeln, wie insbesondere die *Funktion des Aufspürens, der Ortung und Verfolgung* sowie die der *ereignisbezogenen Detektion*, worunter die Feststellung einer (unerwünschten) Veränderung eines definierten Zustandes verstanden wird, wie z.B. bei Einbruchsmeldern oder Radarfallen. Ein staatlicher wie auch privater Einsatz all dieser möglichen Funktionen von RFID ist sowohl durch eine individuelle Überwachung mittels Auslesen als auch unter Verwendung fest installierter Lesegeräte denkbar. So könnten originär zur Überwachung implantierte oder in Pässen, auf Geldscheinen etc. ohnehin vorhandene Transponder etwa für längerfristige Observationen eingesetzt werden, für die sie mindestens eine Vereinfachung sowie Automatisierung bereits vorhandener Möglichkeiten mit sich bringen würden, und ggf. auch die Erstellung von Bewegungsprofilen ermöglichen (vgl. Gräfin von Westerholt/Döring 2004: 710f.). Die begrenzte Reichweite steht der Erstellung von

---

che der Feststellung von Normverstößen und solche der Identifizierung, Ortung etc. angesichts der Überschneidungen beider Bereiche hier nicht weiter verfolgt wird.

8 So wird die Technik bspw. versuchsweise bei der Metro Group im „Future Store" in Rheinberg (<www.future-store.org>) sowie im Rahmen eines Pilotprojekts beim Otto-Versand eingesetzt.

9 Durch den Aufbau eines kaufhausinternen oder global koordinierten Datenbanknetzes erfolgt die konkrete Datenzuweisung, mittels derer weitere – vor allem für die interne Verkaufsoptimierung bestimmte – Informationen den einzelnen Waren und gegebenenfalls ihrem Käufer zugeordnet werden können.

10 So haben BSI und BKA am Flughafen Frankfurt das Biometrieprojekt „BioP II" mit 2000 Testpersonen durchgeführt, bei dem RFID im Rahmen der Identifizierung zum Einsatz kommt. Bei den Tickets für die Fußballweltmeisterschaft 2006 in Deutschland werden RFID-Chips auf den Eintrittskarten persönliche Daten speichern, vgl. <http://www.heise.de/newsticker/meldung/43645>.

Bewegungsprofilen grundsätzlich nicht entgegen. So besteht die Möglichkeit, die Lese- und Schreibeinheiten an bestimmten – für die konkrete Überwachung wesentlichen – Stellen zu positionieren und so ein profil- und geschehensbezogenes Muster zu erstellen. Hierfür käme ein Anbringen beispielsweise an Plätzen in Betracht, denen eine erhöhte Frequenz von Straftatenbegehung zugeschrieben wird. Als ereignisbezogene Detektion über die Identifizierungsfunktion hinaus lässt sich bspw. eine erweiterte Zugangs- bzw. Aufenthaltsregulierung im Sinne einer ortspezifischen Prävention klassifizieren.[11] Hier wird etwa die (vermehrte) Nutzung der Chips in Justizvollzugsanstalten zur Vereinfachung und Intensivierung der Kontrolle abgrenzbarer Bereiche erwogen.

Über eine anderweitige Umsetzung der Regulierungsmöglichkeiten wird mitunter aus dem Ausland berichtet: So würden in Japan Schüler zum Teil mit RFID-Tags ausgerüstet, um auf diese Art deren Bewegungsfreiheit einzuschränken bzw. abweichende Bewegungsmuster zu registrieren und den mit der Erziehung befassten Personen zur Kenntnis zu bringen. Dabei sollen die Chips vor allem zur Anwesenheitskontrolle, Sicherung des Verbleibs auf dem Schulgelände bzw. dessen rechtzeitigen Erreichens durch Anbringen von Lesegeräten an den Schultoren genutzt werden, aber auch zur „Sicherung" bezüglich auf dem Schulweg als gefährlich eingeschätzter Orte (vgl. BSI 2004: 72).

3. Funktionen und Einsatzbereiche durch anfallende Daten

Als sich aus den gespeicherten Daten ergebende Funktionen können die *datenbezogene Detektion* (i.S.d. Feststellung von Abweichung durch Auswertung von Daten) und die *Informationserlangung i.e.S.* (vor allem zur Ermittlung bei Gefahren oder zur Strafverfolgung) verstanden werden, wobei eine solche Überwachung und Kontrolle sowohl mittels Auswertung (noch) auf einem einzelnen Chip gespeicherter Informationen als auch in Datenbanken erfasster Daten in Betracht kommt.

Hier steht im wirtschaftlichen Bereich aufgrund der sich aus dem Einsatz in der Logistik ergebenden Möglichkeiten insbesondere die Optimierung von Verkaufsstrategien im Mittelpunkt des Interesses: Durch die Zuordnung produktspezifischer Daten zu bestimmten Personen oder Personengruppen können Konsum- und Verhaltensprofile zur Nutzung im Marketingbereich erstellt werden,[12] was aus datenschutzrechtlicher Sicht bereits als bedenk-

---

11 Zu Testläufen mit unter die Haut implantierten Speicherchips in Mexiko (vgl. <http://www.heise.de/tp/deutsch/inhalt/te/17867/1.html>).

12 In diesem Bereich kommt bspw. ein Einsatz in Verbindung mit Kundenkarten in Betracht, wobei sich die nicht personenbezogenen Daten auf den Produkt-Chips mit den Daten der Kundenkarte verbinden lassen; vgl. hierzu die rechtlichen Beschränkungen der §§ 4, 6c, 9 BDSG. Ein weiteres Beispiel bildet die von Tesco (Großbritannien) und Wal Mart (USA) vorgenommene Verknüpfung von RFID mit einem Video- oder Fotoaufnahmegerät, welches durch das Ergreifen eines speziellen Pro-

lich zu bewerten ist.[13] Darüber hinausgehend werden sich mit der zunehmenden Verbreitung von RFID aus den Daten weitere Informationen ermitteln lassen, die nicht mehr alleine die Herstellungs- bzw. Erwerbsmodalitäten mit sich geführter Gegenstände betreffen; soweit die Verwendung von RFID in Zukunft nahezu alle Lebensbereiche betrifft, werden sich damit ausgeprägte Persönlichkeitsprofile erstellen lassen. Anzeichen hierfür ist bspw. die berichtete Zulassung eines unter die Haut implantierten RFID-Chips als medizinischem Datenspeicher durch die US-Arzneimittelbehörde für die Vermarktung.[14]

Alleine diese Funktionen des RFID-Einsatzes eröffnen umfassende Möglichkeiten der Ausforschung schon wegen des angestrebten Umfangs, in dem die Chips in Zukunft zum Einsatz kommen sollen: Die millimetergroßen Speicher würden in jedem Lebensbereich vorhanden sein und so zu einem riesigen Datenpool, aus dem Exekutive wie auch Private schöpfen könnten. Als besonders problematisch – weil verschiedene Informationen über eine Person verbindend – erweist sich dabei die Kombination von verschiedenen Funktionen in einem Chip bzw. die Funktionsverknüpfung mit anderen Kontrolltechniken.[15]

4. Zusammenfassung

Die Einsatzmöglichkeiten der RFID-Technologie sind letztendlich unbegrenzt, so dass ihre Funktion und ihr Einsatz für Kontrolle und Überwachung heute nur eingeschränkt beurteilt werden können. Immerhin wird bereits jetzt die Verwendung z.B. auf Geldscheinen, Ausweisen, Eintrittskarten, Nummernschildern[16] und (für Zugangskontrollen) sogar eine Implantierung unter die Haut evaluiert bzw. eingesetzt. Dabei werden Funktionen von Überwachung und Kontrolle sowohl durch die Verbindung der auf dem Chip gespeicherten Daten mit einem Objekt (Identifizierung, Ortung, ereignisbezogene Detektion), als auch durch die sich damit ausbreitende bloße Speicherung anfallender Daten (datenbezogene Detektion, Informationsge-

---

duktes aktiviert wird und auf diese Weise Daten über potentielle Interessenten sammelt (vgl. The Guardian vom 19.07.2003; Chicago Sun Times vom 09.11.2003).

13 Der Bundesbeauftragte für den Datenschutz hat vor diesem Hintergrund eine Erweiterung des BDSG gefordert (vgl. Frankfurter Rundschau vom 07.09.2004). Vgl. auch das Positionspapier des FoeBuD e.V. über den Gebrauch von RFID auf und in Konsumgütern vom 14. bzw. 19.11.2003.

14 Vgl. <http://stern.de/computer-technik/technik/index.html?id=532271&nv=cp_L1_aa>.

15 Gekoppelt bspw. mit einem Videoaufnahmegerät ermöglicht RFID etwa die Anfertigung von Überwachungsbildern bei gehäuftem Auftreten einer bestimmten Kennung und einer entsprechenden Zuschreibung zu einer konkreten Person. Ein Studentenausweis mit einem solchen Chip z.B. soll dann nicht nur zur Verwaltung, sondern auch als Semesterticket, Mensa-Karte etc. dienen; darüber hinaus ist eine Zugangsregulierung sowie die Abrechung von Studiengebühren denkbar.

16 Vgl. <http://www.e-plate.com>.

winnung) bedient, so dass die beiden eingangs genannten Aspekte der technischen Entwicklung durch RFID erheblich berührt sind.

III. Kriminologische Betrachtung

Kriminologische Aspekte des Einsatzes von RFID betreffen zunächst den damit zum Ausdruck kommenden Wandel sicherheitspolitischer Konzepte und sodann Entwicklungen im Bereich von Exekutive und klassischer Kriminalitätskontrolle.

1. Wandel des sicherheitspolitischen Paradigmas

a) Von der Sanktionierung zum Netz aus Kontrolle und Überwachung

Verhaltenskontrolle unterliegt einem grundlegenden Wandel im Sinne einer Ökonomisierung der Steuerungsinstrumente, den man durchaus als schleichenden Paradigmenwandel qualifizieren kann. So scheint sich das Verständnis und die Rolle von staatlicher Überwachung und Kontrolle in der Bevölkerung verändert zu haben, so dass diese eher als Schutz denn als Bedrohung aufgefasst werden; gleichzeitig wird ein gewisser Gewöhnungseffekt zu konstatieren sein (Garland 2004: 36ff., 61ff. m.w.N.; Nogala 2001). Kriminalität und (negativ sanktioniertes) abweichendes Verhalten werden diesem Wandel folgend immer mehr als allgegenwärtige Risiken verstanden, die es präventiv zu kontrollieren und somit zu verwalten gilt. Entsprechend stehen nicht mehr alleine Normen, ihre Einhaltung und die Sanktionierung bei Verstößen, sondern ebenso die Verwaltung des empirisch Normalen durch Techniken der Sicherheit im Mittelpunkt von Verhaltenskontrolle (Lemke/Krasmann/Bröckling 2000: 13ff.).

Ein weiteres Merkmal dieser Entwicklung ist die zunehmende Beteiligung Privater an der Produktion von Sicherheit und zwar sowohl als Anbieter wie auch als Nachfrager (zur „Kustodialisierung" vgl. Elsbergen 2004), zumal sich hier die Möglichkeiten angesichts des technischen Fortschritts und der neuen Kontrollformen vervielfacht haben. Dabei mag die Art der unmittelbaren Reaktion differieren; gleichwohl sind die längerfristigen gesellschaftlichen Folgen privater und staatlicher Kontrolle mindestens ähnlich und nähern sich beide Bereiche angesichts der steigenden Privatisierung von Sicherheit und deren Produktion an. Entsprechend lässt sich auch die Nutzung der RFID-Technik mit ihren Formen und Funktionen auf beiden Seiten finden. Im Ergebnis entwickelt sich daraus eine dezentrale Vielfalt kleiner und großer Kontrollsysteme von Staat, Wirtschaft und Privaten, die neben die disziplinierende staatliche Überwachung treten. Zusammengenommen verdichten sich all diese Techniken der verschiedenen Akteure auf den verschiedenen Ebenen zu einem vielfältigen Netz umfangreicher Verhaltenskontrolle (Nogala 2001).

b) Neue Techniken als Verstärker gesellschaftlichen Konformitätsdrucks

Diese erörterten neuen Formen räumlicher und technischer Kontrolle von als risikoträchtig eingeschätzten Personen bzw. Situationen – wie sie auch durch RFID ermöglicht werden – sind auf eine Manipulation von Verhalten als subtiler Erzeugung und Verinnerlichung von Anpassung an bestimmte Verhaltensanforderungen gerichtet, die zudem Bereiche betreffen, die weit im Vorfeld strafrechtlicher Relevanz liegen. Gerade durch die Möglichkeit und den Einsatz solcher neuen Formen von Kontrolle findet wiederum eine *Ausweitung* des Spektrums von *Gefahren* und *Risiken* in diesem Vorfeld (Krasmann 2003: 45ff.) und damit einhergehend rechtlich eine Loslösung staatlicher Überwachung von herkömmlichen Verdachtselementen oder auch nur von konkreten Anlässen statt, die nicht bei der Zunahme von Vorfeldermittlungen und der Verlagerung von Eingriffsbefugnissen in den präventiven Bereich stehen bleibt, sondern die Perspektive einer potentiell ubiquitären Ausforschung aufscheinen lässt (vgl. Albrecht 2002: 153f., 156 m.w.N.). Die oben aufgezeigten Funktionen und Einsatzbereiche von RFID können als Ausdruck dieses gewandelten Konzepts verstanden werden, wobei sie sowohl für Formen der Überwachung als auch der Kontrolle in Betracht kommen.

Als konkretes Beispiel für das Entstehen solcher Techniken, die an die steigende Bedeutung gespeicherter Daten oder die Entwicklung neuer technischer Möglichkeiten anknüpfen, kann einerseits der automatische Kfz-Kennzeichen-Abgleich angeführt werden[17], der an Autobahnen auch mittels der Verfahren zur Mautregistrierung möglich sein soll; zum anderen sei hier die (ausgeweitete) Ermächtigung zahlreicher Behörden zur Abfrage von Kontodaten aller Bürger beim Bundesamt für Finanzdienstleistungsaufsicht genannt.[18]

Die mit dieser Entwicklung verbundene Verlagerung von Selektionsmacht auf die Exekutive führt zu einer Ausweitung von Konformitätszwang in der Weise, dass nicht nur strafrechtliche sondern Verhaltensanforderungen insgesamt exekutiert werden. Bei den Kontrolltechniken ist dies bereits Bestandteil des Konzepts, im Bereich von Strafrecht und Überwachung eine Folge: Wer sich im Widerspruch zu – auch niedrigschwelligen – sozialen Normen verhält, läuft – noch mehr, als gemäß traditioneller Disziplinierungsfunktionen ohnehin (dazu Eisenberg 2005: § 10, Rn. 20ff., § 53, Rn. 10ff.) – Gefahr, gemäß (nicht nur) polizeilicher Verdachts- und Kontrollstrategien in den strafrechtlichen Selektionsprozess zu geraten.

17 Dieser wird ermöglicht bspw. in Hessen durch das Gesetz über die öffentliche Sicherheit und Ordnung in der geänderten Fassung vom 15.12.2004, GVBl. I: 444.

18 So das Gesetz zur Förderung der Steuerehrlichkeit vom 23.12.2003, BGBl I: 2928.

c) Das Potential von RFID in diesem Konzept

Zusammenfassend betrachtet ist die RFID-Technik mit ihren bisherigen Einsatzfeldern nicht nur *Ausdruck* dieses gewandelten Konzepts von Verhaltenskontrolle. Sie bietet darüber hinaus auch ein erhebliches *Potential*, d.h. jedenfalls die Eigenschaften und daraus folgend die Einsatzmöglichkeiten, für verschiedenste Formen der Überwachung und Kontrolle durch Staat und Private. Dies gilt sowohl bei der Auswertung gespeicherter Datenmassen als auch für den Einsatz als neue Technologie bei neuen Kontrollformen. Die besondere Bedeutung von RFID liegt dabei einerseits in der Allgegenwärtigkeit einer automatischen Abfrage und Speicherung von Daten des täglichen Lebens. Diese Neuartigkeit i.S.d. ubiquitären Computings ist dabei durch die Effizienz i.S. hoher Leistungsfähigkeit, der sich aus einer Miniaturisierung ergebenden Unauffälligkeit und den Möglichkeiten der Vernetzung der Systeme bestimmt. Zum anderen ist die RFID-Technik, wie oben dargelegt, in der Lage, Formen für sehr verschiedene Funktionen von Kontrolle und Überwachung zu bedienen und diese sogar in einer Technik zu verbinden.

Gleichwohl bestehen auch Unwägbarkeiten bezüglich der technischen Umsetzung und insbesondere der Frage, wie die dann anfallenden Datenmassen handhab- und auswertbar gemacht werden können.[19] Dennoch ist aber von einem zunehmenden Einsatz insbesondere solcher Mittel auszugehen, die eine Stärkung des Sicherheitsgefühls erzeugen, um entsprechenden Bedürfnissen und einem in Teilen gewandelten Verständnis von Kontrolle und Überwachung Rechnung zu tragen. Inwieweit die konkrete Umsetzung eine reale Auswirkung auf bestehende Gefahrenpotentiale hat, mag dabei zweitrangig sein.

2. Befugnis- und Machtverschiebung exekutiver Staatsorgane (Verpolizeilichung)

Die Ausweitung von Kontrolle und Überwachung ebenso wie der steigende Einsatz von heimlichen Ermittlungsmethoden (vgl. Rzepka 2000: 426f.) bringen eine so genannte „Verpolizeilichung" nicht nur des Strafverfahrens, sondern staatlicher Verhaltenskontrolle insgesamt mit sich. Dies folgt unstreitig daraus, dass der Einsatz solcher Maßnahmen aufgrund der rechtlichen Zuordnung und der personellen wie technischen Gegebenheiten zu einem dominierenden Hauptteil von Institutionen der Exekutive durchgeführt, durch Beantragung initiiert sowie in vielen Fällen auch direkt angeordnet wird (vgl. schon Nelles 1980: 227; Asbrock 1997: 258). Eine Ausdehnung solcher Maßnahmen (zur Telekommunikationsüberwachung Albrecht/

19 So sei bspw. Anfang des Jahres 2005 die Planung für die Einführung von auf RFID-Chips gespeicherten biometrischen Merkmalen in Visa und Pässe der EU-Länder aufgrund von Problemen bei der technischen Umsetzung ins Stocken geraten (vgl. <http://www.heise.de/newsticker/meldung/54879>).

Dorsch/Krüpe 2003: 30) bedeutet somit einen weitergehenden *Zuwachs* der tatsächlichen Kompetenzen der *Exekutivorgane* und im besonderen Maße der Polizei. Dies gilt umso mehr, da technische Mittel – wie potentiell auch RFID – häufig dazu genutzt werden, *heimliche* Überwachungen vorzunehmen. Zwar unterliegen viele Formen einer solchen Überwachung einem Richtervorbehalt (vgl. exemplarisch §§ 100b Abs.1 und 100d Abs. 4 Satz 1 StPO), jedoch ist die Kontrollfunktion durch die informatorische Abhängigkeit der Gerichte von den tatsächlich ermittelnden Behörden und ggf. bestehende organisatorische Defizite eingeschränkt (Kühne 2003: Rn. 410; bzgl. Telefonüberwachung Backes/Gusy 2003: 45ff.). Weitere Beschränkungen ergeben sich durch den Mangel an rechtlichen Abwehrmöglichkeiten auf Seiten der Betroffenen: Während nicht-heimliche Maßnahmen regelmäßig sofort in Form der Beschwerde auf ihre Rechtmäßigkeit überprüft werden können, steht einem von heimlicher Überwachung Betroffenen dieses Mittel mangels frühzeitiger Kenntnis nur eingeschränkt zur Verfügung.

Mitunter scheinen Organe der Exekutive an dieser Verschiebung von Befugnissen selbst als maßgebliche Akteure beteiligt zu sein. Dafür spricht nicht zuletzt die Historie von rechtlichen Abgrenzungs- und Subsumtionsschwierigkeiten betreffend neue Überwachungstechnologien, die zu einer der abschließenden rechtlichen Würdigung zuvorkommenden Anwendung in der Praxis führt, die sodann ggf. eine Schaffung von Rechtsgrundlagen erst nach sich zieht (vgl. Wolter 2004: 743f.). Insofern ist eine sich verselbständigende – außerhalb ausdifferenzierter rechtlicher Vorgaben erfolgende – Überwachungspraxis nicht etwa erst aufgrund der Möglichkeiten der RFID-Technologie zu besorgen, sondern erweist sich als ein dem staatlichen Umgang mit technischer Entwicklung inhärentes Phänomen, das zum Teil auch auf das Wirken institutionalisierter Handlungsnormen (vgl. hierzu Eisenberg 2005: § 40; speziell zu solchen bei Staatsanwaltschaften vgl. Singelnstein 2003) zurückgeführt werden kann.

Indes bezieht sich RFID im Unterschied zu bisherigen Technologien bei Kontrolle und Überwachung nicht auf einzelne (zum Teil eng abgrenzbare) Lebensbereiche, sondern bietet die Möglichkeit einer einfachen Informationsgewinnung auf nahezu allen Ebenen des Privatlebens – bei einer lediglich mittelbaren Nutzung ähnlich der Bewegungsprofilerstellung durch Mobilfunkgeräte auch ohne vorheriges Handeln seitens staatlicher Organe (hierzu Eisenberg/Singelnstein 2005: 62ff.). Insbesondere in der Kombination mit anderen Ermittlungsmethoden – etwa Videoüberwachung oder GPS–Technologie – und aufgrund des Umfangs der in Rede stehenden Datenmengen ergibt sich eine Qualität der Überwachungsmöglichkeiten, die aus polizei- und strafverfolgungsbehördlicher Sicht eine folgerichtige Weiterentwicklung der Eingriffsinstrumente darstellen mag, jedoch aus rechtstaatlicher Sicht ein erhebliches *Bedrohungspotential* aufweist (vgl. auch Wolter 2004: 745).

3. Effizienzfortschritt bei der Kriminalitätsbekämpfung durch Technik?

Im Bereich der herkömmlichen Überwachung zwecks Kriminalitätskontrolle wird die Nutzung technischer Mittel und insbesondere auch neuer Technologien zur operativen Ermittlung vor allem mit der Notwendigkeit eines Eindringens in nach außen abgeschottete „kriminelle Strukturen", etwa im Bereich des so genannten „Organisierten Verbrechens" oder (staatsführungsbekämpfender) terroristischer Organisationen begründet (vgl. BT-Drs. 12/989: 21). Bereits dieser Zielsetzung treten indes Bedenken bezüglich der begrifflichen Unbestimmtheit und des tatsächlichen Ausmaßes solcher Erscheinungsformen gegenüber (vgl. BVerfG NJW 2004: 1009; Eisenberg 1993: 1033ff.; Kinzig 2004: 704ff., 775ff.). Weiterhin gehen solche Konzepte grundsätzlich fehl, soweit sie die betreffende Ausweitung mit der Notwendigkeit einer technischen Anpassung der Strafverfolgungsbehörden an etwaige Möglichkeiten zur Deliktbegehung begründen. Zwar mögen in Einzelfällen, etwa bei inhaltsbezogener Telekommunikationsüberwachung, entsprechende Erwägungen tragen. Eine Vielzahl dieser Maßnahmen[20] – inklusive einer möglichen Nutzung von RFID – betreffen hingegen gerade nicht ein Sich-Einstellen auf veränderte Begehungsweisen durch technischen Fortschritt, sondern dienen vielmehr der Intensivierung und Rationalisierung der Kontrolle von Verhaltensweisen im Allgemeinen. Insbesondere scheint die einfache und automatisierte Anwendung ein bedeutender Gesichtspunkt bei der Entscheidung für eine bestimmte heimliche Ermittlungsmethode zu sein. So sollen die überaus geringen Anwendungszahlen bei der akustischen Wohnraumüberwachung – gerade im Verhältnis zur Telekommunikationsüberwachung – wesentlich auch mit dem erheblichen Aufwand und praktischen Problemen bei der Umsetzung zusammenhängen (Meyer-Wieck 2004: 146 ff).

Dieses Bestreben nach Effektivierung einer allgemeinen Verhaltenskontrolle zeigt auch das Ausmaß der in Kauf genommenen *Überwachung von Nichtverdächtigen* – selbst wenn man die Erforderlichkeit sowie eine Erreichbarkeit der offiziell angestrebten Ziele unterstellen würde. So ist eine relativ geringe unmittelbare Relevanz einzelner technischer Maßnahmen für das konkrete Ermittlungsverfahren z.B. für die akustische Wohnraumüberwachung nachgewiesen (vgl. BT-Drs. 14/8155: 22ff.; zur Telekommunikationsüberwachung Albrecht/Dorsch/Krüpe 2003: 371). Einem bei heimlichen technischen Ermittlungsmaßnahmen eher hohen Anteil *betroffener Unbeteiligter* stehen indes verdächtige Personen und Personengruppen gegenüber, die durchaus bestrebt und in der Lage sein werden, sich der Überwachung zu entziehen (vgl. Meyer-Wieck 2004: 128f.) – bzgl. RFID bspw.

20 Dies betrifft bspw. die akustische Gesprächsüberwachung, Observation mit technischen Mitteln, Einsatz eines GPS-Senders, die Verwendung eines IMSI-Catchers zur Standortbestimmung, die Nutzung von Mobilfunkdaten zur Standortbestimmung, Rasterfahndung.

durch Einsatz von Blockern oder ähnlichen Abwehrmaßnahmen. Somit wären es gerade Unbeteiligte, die einem besonders hohen Risiko einschlägiger Eingriffe unterworfen sind.

IV. Ausblick

Die RFID-Technik ist eingebettet in ein – auch andere Techniken einbeziehendes – ubiquitäres Computing als einer immer umfassender werdenden Datensammlung und -speicherung in allen Lebensbereichen, jedoch wohnt ihr für die in Rede stehende Thematik ein besonderes Steigerungspotential inne. Rechtspolitisch wären zumindest aus datenschutzrechtlicher Sicht eine Hinweispflicht sowie Vorkehrungen nötig, die dem Datenvermeidungsgebot des § 3a BDSG gerecht werden.[21] Im technischen Bereich sind mindestens eine Beschränkung der Funktionalität der RFID-Chips auf das für die jeweilige Funktion notwendige Maß sowie die automatische Deaktivierung nach Funktionserfüllung angezeigt. Hierzu existieren bereits entsprechende Technologien und – die Verantwortung indes auf den Verbraucher abschiebende – Vorhaben (Langheinrich 2004). Jedoch erscheint eine Herbeiführung der Funktionsunfähigkeit alleine durch Kunden selbst keinen ausreichenden Schutz zu bieten. Insbesondere bestehen mögliche Anreize auch der privat initiierten weitergehenden Nutzung der Tags bspw. zur Erkennung und Wiederbeschaffung gestohlenen Eigentums, wodurch ein Risikobewusstsein möglicherweise verdrängt wird. Schließlich begegnet ein System der Verhaltenskontrolle, das sehr frühzeitig und niedrigschwellig mit subtil und manipulativ wirkenden Methoden agiert, grundlegenden gesellschaftspolitischen Einwänden.

Literatur

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane (2003): Rechtwirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg i.Br.

Albrecht, Peter-Alexis (2002): Kriminologie, 2. Aufl., München.

Asbrock, Bernd (1997): Zum Mythos des Richtervorbehalts als wirksames Kontrollinstrument im Zusammenhang mit besonderen polizeilichen Eingriffsbefugnissen, in: Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 80, S. 255-262.

Backes, Otto/Gusy, Christoph (2003): Wer kontrolliert die Telefonüberwachung?, Frankfurt a.M.

Bär, Wolfgang (2000): Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, in: Multimedia und Recht 3, S. 472-480.

21 So auch die Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.3.2004 (vgl. <http://www.lfd.m-v.de/beschlue/ent67.html>).

Bundesamt für Sicherheit in der Informationstechnik (2004): Risiken und Chancen des Einsatzes von RFID-Systemen, Bonn.
Demko, Daniela (2004): Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme, in: Neue Zeitschrift für Strafrecht 24, S. 57-64.
Dreier, Horst (2004): Grundgesetz, 2. Aufl., Tübingen.
Eisenberg, Ulrich (1993): Straf(verfahrens-)rechtliche Maßnahmen gegenüber „Organisiertem Verbrechen", in: Neue Juristische Wochenschrift 46, S. 1033-1039.
Eisenberg, Ulrich (2002): Beweisrecht der StPO, 4. Aufl., München.
Eisenberg, Ulrich (2005): Kriminologie, 6. Aufl., München.
Eisenberg, Ulrich/Puschke, Jens/Singelnstein, Tobias (2005): Überwachung mittels RFID-Technologie, in: Zeitschrift für Rechtspolitik 38, S. 9-12.
Eisenberg, Ulrich/Singelnstein, Tobias (2005): Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS", in: Neue Zeitschrift für Strafrecht 25, S. 62-67.
Elsbergen, Gisbert van (2004): Das Konzept der Kustodialisierung – Innere Sicherheit zwischen staatlicher Kontrolle und Privatisierung, in: Elsbergen, Gisbert van (Hrsg.): Wachen, kontrollieren, patrouillieren, Wiesbaden, S. 13-29.
Garland, David (2004): Die Kultur der „High Crime Societies", in: Oberwittler, Dietrich/Karstedt, Susanne (Hrsg.): Soziologie der Kriminalität, Wiesbaden, S. 36-68.
Hansen, Marit/Wiese, Markus (2004): RFID – Radio Frequency Identification, in: Datenschutz und Datensicherheit 22, S. 109.
Kinzig, Jörg (2004): Die rechtliche Bewältigung von Erscheinungsformen Organisierter Kriminalität, Berlin.
Krasmann, Susanne (2003): Gefährdungsausweitung – Die Kriminologie und die Transformation des Sozialen, in: Pieper, Marianne/Guitiérez Rodríguez, Encarnación (Hrsg.): Gouvernementalität, Frankfurt a.M., S. 39-49.
Kühne, Hans-Heiner (2003): Strafprozessrecht, 6. Aufl., Heidelberg.
Langheinrich, Marc (2004): Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, o.O.
Lemke, Thomas/Krasmann, Susanne/Bröckling, Ulrich (2000): Gouvernementalität, Neoliberalismus und Selbsttechnologien, in: Bröckling, Ulrich/Krasmann, Susanne/Lemke, Thomas (Hrsg.): Gouvernementalität der Gegenwart, Frankfurt a.M., S. 7-40.
Meyer-Goßner, Lutz (2004): Strafprozessordnung, 47. Aufl., München.
Meyer-Wieck, Hannes (2004): Rechtwirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff") nach § 100c Abs. 1 Nr. 3 StPO, Vorausversion, Freiburg i.Br.
von Münch, Ingo (2000), in: von Münch, Ingo/Kunig, Philip (Hrsg.): Grundgesetz Kommentar, 5. Aufl., München.
Nack, Armin (2003): §§ 94-111p, in: Pfeiffer, Gerd (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung, 5. Aufl., München.
Nelles, Ursula (1980): Kompetenzen und Ausnahmekompetenzen in der Strafprozessordnung, Berlin.

Nogala, Detlef (2001): Der Frosch im heißen Wasser, in: Schulzki-Haddouti, Christiane (Hrsg.): Vom Ende der Anonymität, 2. Aufl., Hannover, S. 139-155.

Puschke, Jens (2005): Die kumulative Anordnung von Informationsbeschaffungsmaßnahmen im Rahmen der Strafverfolgung, Diss., Berlin.

Rzepka, Dorothea (2000): Zur Fairness im deutschen Strafverfahren, Frankfurt a.M.

Singelnstein, Tobias (2003): Institutionalisierte Handlungsnormen bei den Staatsanwaltschaften im Umgang mit Ermittlungsverfahren wegen Körperverletzung im Amt gegen Polizeivollzugsbeamte, in: Monatsschrift für Kriminologie und Strafrechtsreform 86, S. 1-26.

Westerholt, Margot Gräfin von/Döring, Wolfgang (2004): Datenschutzrechtliche Aspekte der Radio Frequency Identification – Ein „Virtueller Rundgang" durch den Supermarkt der Zukunft, in: Computer und Recht 20, S. 710-716.

Wolter, Jürgen (2004): Potential für eine Totalüberwachung im Strafprozess- und Polizeirecht, in: Rogall, Klaus (Hrsg.): Festschrift für Hans-Joachim Rudolphi zum 70. Geburtstag, Neuwied, S. 733-748.

Fachbereich Rechtswissenschaft, Freie Universität Berlin, Van't-Hoff-Str. 8, 14195 Berlin