

Politik, Prävention, Privatheit: Orwell und die britische Gegenwart

Andreas Busch

Die fürchterlichste Dystopie des totalen Überwachungsstaates ist wohl auch heute noch die, die der britische Schriftsteller George Orwell in der zweiten Hälfte der 1940er Jahre in einen Roman gefasst hat.¹ Es vergeht kaum ein Gespräch über oder eine Stellungnahme zum Thema „Überwachung“, ohne dass die dem Titel dieses Buches geschuldete Zahl genannt wird: „1984“. Das damit assoziierte Jahr ist bereits seit einem Vierteljahrhundert vergangen; aber bevor dieser Artikel sich seinem Hauptthema, nämlich einer Diskussion des Zusammenhangs zwischen Politik, Prävention und Privatheit am Beispiel der britischen Gegenwart zuwendet, sollen einige Passagen aus Orwells Buch über den totalitären Staat Ozeanien, der seine Untertanen durch allgegenwärtige Überwachung zum Gehorsam zwingt, das Leben der Hauptfigur des Romans, Winston Smith, noch einmal vergegenwärtigen.

„Die Welt draußen sah selbst durch die geschlossenen Fenster kalt aus. Unten auf der Straße wirbelten schwache Windstöße Staub und Papierfetzen in Spiralen hoch, und obwohl die Sonne strahlte und der Himmel leuchtend blau war, schien doch alles farblos, außer den überall angebrachten Plakaten. Das Gesicht mit dem schwarzen Schnurrbart blickte von jeder beherrschenden Ecke herunter. Ein Plakat klebte an der unmittelbar gegenüberliegenden Hausfront. 'Der Große Bruder sieht dich an!' hieß auch hier die Unterschrift, und die dunklen Augen bohrten sich tief in Winstons Blick. [...] In der Ferne glitt ein Helikopter zwischen den Dächern herunter, brummte einen Augenblick wie eine Schmeißfliege und strich dann in einem Bogen wieder ab. Es war die Polizeistreife, die den Leuten in die Fenster schaute. Die Streifen waren jedoch nicht schlimm. Zu fürchten war nur die Gedankenpolizei.

Hinter Winstons Rücken schwatzte die leise Stimme aus dem Televisor noch immer von Roh-eisen und von der weit über das gesteckte Ziel hinausgehenden Erfüllung des neunten Dreijah-resplans. Der Televisor war gleichzeitig Empfangs- und Sendegerät. Jedes von Winston verursachte Geräusch, das über ein ganz leises Flüstern hinausging, wurde von ihm registriert. Außerdem konnte Winston, solange er in dem von der Metallplatte beherrschten Sichtfeld blieb, nicht nur gehört, sondern auch gesehen werden. Es bestand natürlich keine Möglichkeit, fest-zustellen, ob man in einem gegebenen Augenblick gerade überwacht wurde. Wie oft und nach welchem System die Gedankenpolizei sich in einen Privatapparat einschaltete, blieb der Mut-maßung überlassen. Es war sogar möglich, daß jeder einzelne ständig überwacht wurde. Auf alle Fälle aber konnte sie sich, wenn sie es wollte, jederzeit in einen Apparat einschalten. Man mußte in der Annahme leben – und man stellte sich tatsächlich instinktiv darauf ein –, daß je-

- 1 Dieser Aufsatz wurde verfasst während der Autor Fellow am Hanse-Wissenschaftskolleg war. Dem Kolleg gilt mein herzlicher Dank für eine gleichzeitig ruhige und stimulierende Arbeitsumgebung. Die Forschung wurde finanziell durch Grant RES-062-23-0536 des britischen *Economic and Social Research Council* unterstützt, und dem ESRC gilt ebenfalls mein herzlicher Dank.

des Geräusch, das man machte, mitgehört und, außer in der Dunkelheit, jede Bewegung beobachtet wurde“ (Orwell 2000: 6).

George Orwell, der mit bürgerlichem Namen Eric Blair hieß, war einer der führenden britischen Schriftsteller seiner Zeit, der sich – politisch links stehend – unter dem Eindruck der Erfahrung des Stalinismus und seiner expansiven Strategie nach dem Zweiten Weltkrieg stark gegen den Kommunismus und Totalitarismus wandte. Das Buch hatte er im Jahr 1948 geschrieben – und den Titel durch Verdrehung der letzten beiden Ziffern gewählt. Die ikonenhafte Ziffer ist demnach in einem gewissen Maße dem Zufall geschuldet; nicht zufällig (wenn auch in einem umbenannten Großbritannien namens „Airstrip One“ liegend) ist hingegen der Ort, an dem die Handlung spielt: London.

Natürlich ist das London aus Orwells Roman nicht das London von heute, ebenso wenig wie es das von vor 25 Jahren war. Aber Großbritannien wird heute oft (zumindest unter den liberalen westlichen Demokratien) als führend im Bereich der Überwachung angesehen, und auch von offizieller Seite wird das Land bereits als „Überwachungsgesellschaft“ (*surveillance society*) eingestuft.²

Im folgenden Beitrag soll diese Überwachungsgesellschaft beschrieben und analysiert werden. Der Fall Großbritanniens soll dabei in keiner Weise besonders herausgehoben werden – vielmehr steht er *pars pro toto* für das, was technisch und politisch möglich ist in einer liberalen Demokratie, die verwaltungstechnisch hoch entwickelt und hoch zentralisiert ist und über wenig formale und politische Gegengewichte zur Macht der Regierung verfügt. In einem ersten Teil werden (nach einem kurzen Blick auf die Entstehung und Charakteristika des britischen Datenschutzsystems) verschiedene Bereiche der die Privatheit der Bürger betreffenden Überwachungstechniken beschrieben und analysiert. In einem zweiten Teil steht dann das Bemühen um eine Erklärung im Mittelpunkt, warum sich Überwachung in Großbritannien in einem so vergleichsweise starken Maße hat staatlich durchsetzen lassen. Ein Blick auf die Politisierung des Themas in letzter Zeit sowie einige Spekulationen über die zukünftige Entwicklung beenden den Beitrag.

- 2 So urteilt der britische Information Commissioner Richard Thomas im Jahresbericht 2006/07: „The purposeful, routine and systematic recording of everyone’s movements, activities and transactions in public and private spaces – a surveillance society – is fast becoming a reality.“ (Information Commissioner’s Office 2007: 6). Siehe zu einer ähnlichen Einschätzung auch den zweibändigen Bericht des britischen Oberhauses zum Thema Überwachung (House of Lords. Select Committee on the Constitution 2009), zu einer gegenteiligen Einschätzung den Bericht des Innenausschusses des Unterhauses (House of Commons. Home Affairs Committee 2008). In vergleichender Hinsicht siehe die Einstufung durch die Menschenrechtsgruppe *Privacy International* im „2007 International Privacy Ranking“ (Privacy International 2007), die Großbritannien als einziges OECD-Land neben den USA in die niedrigste von insgesamt sieben Kategorien einstuft und es (auf einer Stufe mit Russland, China etc.) als „endemic surveillance society“ bezeichnet. Dieses *ranking* vergleicht etwa 40 Länder und klassifiziert sie nach insgesamt 13 Variablen. Als Beispiel für eine frühe Nutzung des Konzepts „surveillance society“ siehe Flaherty (1989).

1. Überwachung, Datenschutz und der britische Staat

Diskussionen um den Schutz der Privatsphäre des Einzelnen gegenüber der aufkommenden Computertechnologie und ihrer Nutzung im öffentlichen und privaten Sektor hat es in den westlichen Demokratien ab Ende der 1960er Jahre gegeben. Auch in Großbritannien, einem Land, dessen Wertschätzung der Privatsphäre generell als hoch eingestuft wird, war das so. Dennoch ließ eine erste gesetzliche Regelung der neuen Materie in diesem Land länger auf sich warten als in vergleichbaren Ländern wie den USA, Kanada oder den großen westeuropäischen Ländern – obwohl man das Thema früh zu diskutieren begonnen hatte (Bennett 1992: 59). Ein Grund dafür war, dass die beiden prinzipiellen Ansätze, mit denen Politik auf die Herausforderungen der Computerisierung reagieren konnte, jeweils Konflikte mit Grundsätzen der britischen Verfassungswirklichkeit heraufbeschworen: der Weg über die Etablierung individueller Rechte auf Schutz der Privatsphäre (wie er in den USA und Kanada beschritten wurde) hätte die Positivierung von Freiheitsrechten notwendig gemacht und die Rolle der Gerichte massiv erhöht – was als nicht wünschenswert angesehen wurde; andererseits hätte die Einrichtung einer unabhängigen Agentur, die den Informationsgebrauch der britischen Behörden überwachen und einschränken würde (der in den kontinentaleuropäischen Staaten gewählt wurde) angesichts der wenig ausgeprägten Gewaltenteilung im Land – je nach der genauen Verortung im politischen System – entweder Konflikte mit dem Prinzip der Parlamentssoveränität oder mit dem Grundsatz der ministeriellen Verantwortlichkeit heraufbeschworen (Regan 1990). Das Ergebnis dieser komplizierten politischen Gemengelage war ein Kompromiss mit einer vergleichsweise schwachen Institutionalisierung von Datenschutz und einer Betonung von Flexibilität für die Exekutive in den Detailregelungen (Raab 1993: 49). In Verbindung mit der Abwesenheit einer geschriebenen Verfassung waren dem britischen Staat im Hinblick auf den Datenschutz somit insgesamt wenig Hindernisse in den Weg gelegt, moderne Computertechnologie zu Zwecken der Überwachung einzusetzen, falls das für politische Zwecke dienlich erschien.

So sind in den Jahren seit der Verabschiedung des „Data Protection Act of 1984“ in einer Vielzahl von Bereichen enorme Überwachungskapazitäten aufgebaut worden. Zwei dieser Bereiche sollen im Folgenden genauer dargestellt werden, nämlich die Themen *closed circuit television* (CCTV) bzw. Kameras im öffentlichen Raum und die Sammlung und Auswertung von genetischem Material in einer nationalen DNA-Datenbank. Ein kurzer Ausblick auf andere (realisierte und geplante) Überwachungsvorhaben schließt diesen Teil des Beitrages ab.

1.1. CCTV: Kameras im öffentlichen Raum

Vielleicht die bekannteste Form der Überwachung im heutigen Großbritannien (und die evidenteste Parallele mit Orwell's Dystopie) ist die durch Kameras im öffentlichen Raum, auch bekannt unter der Bezeichnung *closed circuit television* oder (ab-

gekürzt) CCTV.³ Großbritannien wird in diesem Bereich als weltweit führend eingestuft und zwar sowohl von akademischen Autoren (etwa Norris/Armstrong 1999: 3; Schröder 2007: 43) wie auch von offizieller Seite (etwa Gerrard 2007: 5) und von verantwortlichen Politikern.⁴

Erste Experimente mit ferngesteuerten Kameras hatte es in Großbritannien bereits in den 1960er Jahren gegeben, doch waren damals die Übertragungskosten für solche Bilder noch prohibitiv hoch (Williams 2003). Auch als Mitte der 1980er Jahre die erste dauerhafte Überwachungsanlage auf der Promenade des Badeortes Bournemouth in Dienst genommen wurde, war das Wachstum zunächst langsam geblieben – Ende der 1980er Jahre gab es lediglich in fünf Stadtzentren CCTV-Systeme (McCahill/Norris 2002). Doch in der ersten Hälfte der 1990er Jahre wurde CCTV binnen kurzer Zeit zur zentralen Kriminalitätsbekämpfungs-Strategie, die die Unterstützung beider großen Parteien genoss. Dies war vor allem drei Entwicklungen bzw. Ereignissen geschuldet, von denen eine die Ausbreitung von CCTV massiv beförderte während die beiden anderen mögliche Hindernisse dagegen neutralisierten bzw. ausschalteten.

Der starke Anstieg der Kriminalitätsstatistiken hatte die konservative Regierung Anfang der 1990er Jahre in eine schwierige Situation gebracht. Trotz deutlicher Erhöhung der Ausgaben für Polizeiarbeit war keine Trendumkehr in Sicht; ein kritischer Bericht der *Audit Commission*, der (unter Verweis auf angebliche Erfolge bei der Verbrechensbekämpfung in der schottischen Kleinstadt Airdrie) den Einsatz von CCTV als Lösung empfahl, konnte unter diesen Umständen große Wirkung entfalten (Audit Commission 1993). Gleichzeitig hatte die Labour Party (nach ihrer vierten Wahlniederlage im Jahr 1992) sich im Zuge des „Left Realism“ einer offensiveren Verbrechensbekämpfung verschrieben („tough on crime, touch on the causes of crime“) und unterstützte die Forderung nach flächendeckender Einführung von CCTV (McCahill/Norris 2002: 11). Und schließlich hatte der im Jahr 1993 das Land tief erschütternde Fall der Ermordung des dreijährigen James Bulger durch zwei zehnjährige Jungen (der durch in einem Einkaufszentrum eingesetzte Kameras zwar nicht verhindert, aber aufgeklärt werden konnte) Widerstand gegen CCTV von bürgerrechtlicher Seite zum Schweigen gebracht (Schröder 2007: 41).

1994 startete die konservative Regierung ein Programm mit einem Volumen von 2 Mio. Pfund, in dem sich Städte um die Ko-Finanzierung von CCTV-Systemen bei der Zentralregierung bewerben konnten. Aufgrund starker Nachfrage (über 480 Bewerbungen) musste das Programm bald auf 5 Mio. Pfund erhöht werden. Dennoch konnte zunächst nur weniger als ein Viertel der Anträge bewilligt werden. Bis 1999 wurden schließlich 38,5 Mio. Pfund bereitgestellt, um 585 Systeme aufzubauen.

3 Zur generellen Einführung in CCTV siehe Norris/Armstrong (1999) sowie (aus kulturwissenschaftlicher Sicht) Kammerer (2008), zu einem Überblick über die Situation in Großbritannien Goold (2004) sowie McCahill/Norris (2002). Einen guten Überblick über die akademische Beschäftigung mit Überwachung (*surveillance studies*) bietet Lyon (2007).

4 Vgl. etwa das Vorwort des Minister of State for Security, Counter Terrorism and Police, Tony McNulty, in Gerrard (2007): 4: „The United Kingdom is generally recognised as a leading user of Closed Circuit Television (CCTV)“.

en. Ab 1999 wurde schließlich für vier Jahre unter dem Namen *Crime Reduction Programme* (CRP) weitere 170 Mio. Pfund für Investitionen in diesem Bereich zur Verfügung gestellt, die den Aufbau von weiteren 684 CCTV-Systemen ermöglichten. Insgesamt wurden so im Lauf eines Jahrzehnts 250 Mio. Pfund an öffentlichen Geldern für Videoüberwachung im öffentlichen Raum aufgewandt und zeitweise vier Fünftel des Budgets für Kriminalprävention in solche Anlagen gesteckt.⁵

Da die Empfehlung für den Einsatz von CCTV-Systemen mit der *Audit Commission* von einer Institution kam, die ihre Existenz dem Denken in *cost-benefit*-Kategorien schuldet, liegt eine erhebliche Ironie in der Tatsache, dass die flächendeckende Einführung dieser Systeme ohne vorhergehende Evaluierung ihrer Wirksamkeit erfolgte:

„It may be thought that the rush to install CCTV during the 1990s was based on a firm foundation of supporting research evidence as to its effectiveness. This was not so. CCTV was introduced in town centres and the government funded the expansion prior to conducting any systematic evaluation of its effectiveness in reducing crime in such locations“ (McCahill/Norris 2002: 15).

Tatsächlich weisen die durchwegs erst *ex post* durchgeführten Evaluationsstudien auf eine höchst mäßige Wirksamkeit des Einsatzes von CCTV bei der Kriminalitätsbekämpfung hin (Gill 2005). Und auf die Frage nach den Belegen für eine Wirksamkeit von CCTV bei der Verhinderung und Aufklärung von Kriminalität antwortete einer der führenden Experten, Prof. Clive Norris vor der Untersuchungskommission des *House of Lords* im Jahr 2008:

„‘Little’ I think is the short answer. When CCTV was first introduced in this country, it was not subject to systematic evaluation. It was introduced on the basis that practitioners thought that it was effective. Over the last ten years, studies have been carried out by academics and particularly the work by Jason Ditton in Glasgow and the work of Professor Martin Gill at the University of Leicester, which suggests overall that it has a very, very weak influence on reducing crime. The Gill study was published in 2004; it was the first major Home Office sponsored evaluation. Not only did it show that CCTV had very limited impact in reducing crime but it had very limited impact in reducing fear of crime. The evidence in terms of general reductions in crime and general reductions in fear of crime appears to be very, very weak“ (House of Lords. Select Committee on the Constitution 2009: vol 2, 26).

Angesichts der fraglichen Wirksamkeit von CCTV bei der Verbrechensbekämpfung stellt sich die Frage nach den negativen „Nebenwirkungen“ in Bezug auf Bürgerrechte natürlich mit umso größerer Dringlichkeit. Doch gegen eine Kombination aus sozialen, wirtschaftlichen und politischen Druckfaktoren, die CCTV als „Lösung“ anpriesen, waren bloße Fakten offenbar von geringem Gewicht (Norris/Armstrong 1999: 205ff. ; Lyon 2007: 39f.).

5 Angaben nach Norris/Armstrong (1999: 35ff.); McCahill/Norris (2002); Schröder (2007: 44) und Gerrard (2007: 7).

1.2. Die nationale DNA-Datenbank

Ist der britische Staat (inklusive der Städte und Kommunen) angesichts der Überzahl von Kameras im privaten Sektor nur ein Spieler unter anderen beim Thema visuelle Überwachung – wenn auch ein entscheidender, da er ja bewusst den Bereich keiner einheitlichen gesetzlichen Regulierung unterwirft –, so steht er beim Thema „Bioinformation“ allein in der Verantwortung.⁶

Die britische *National DNA Database* oder NDNAD wurde 1995 in England und Wales begründet.⁷ Großbritannien war damit eines der ersten Länder, das eine solche Datenbank einführt (Interpol DNA Unit 2003: 17), und es gehört zu den „strategischen Zielen“ des Innenministeriums, die „weltweit führende Rolle“ der NDNAD zu erhalten.⁸ Weltweit führend ist die NDNAD fraglos hinsichtlich ihrer schieren Größe in Proportion zur Bevölkerung: 7,4% der Bewohner Großbritanniens waren im Januar 2009 in der NDNAD erfasst (House of Lords. Select Committee on the Constitution 2009: vol 1, S.43). Um die bisher erfassten knapp 4,5 Mio. DNA-Proben in der Datenbank zu sammeln (pro Jahr kommen gegenwärtig etwa 700.000 hinzu), sind die Hürden für einen Eintrag sehr niedrig gehalten:⁹ So kann jedem, der über 10 Jahre alt ist und wegen einer *recordable offence* festgenommen wird, sofort eine DNA-Probe entnommen werden. Diese wird auch dann nicht wieder aus der Datenbank gelöscht, wenn der Festgenommene nicht angeklagt oder freigesprochen wird. Dabei ist die Zahl der *recordable offences* in den letzten Jahren stark gestiegen: umfasste sie 1997 alle mit einer Freiheitsstrafe bedrohten Vergehen sowie fünf weitere, ist letztere Zahl mittlerweile auf 52 erhöht worden und umfasst mittlerweile auch Vergehen wie hartnäckiges Betteln und unlizenzirtes Taxifahren (Nuffield Council on Bioethics 2007: 10).

Ähnlich wie im Fall der Videoüberwachung hat auch bei der Nationalen DNA-Datenbank die Finanzierung durch den britischen Zentralstaat zum massiven Wachstum beigetragen. War die Datenbank in den ersten fünf Jahren ihres Bestehens mit jährlich etwa £19 Mio. aus dem Budget der Polizei finanziert worden und in dieser Zeit auf 750.000 Proben angewachsen, so wurde im April 2000 das *DNA Expansion Programme* aufgelegt, das eine zentrale Finanzierung von £182 Mio. über vier Jahre bereitstellte und somit die erhältlichen Mittel mehr als verdoppelte. Im Haushaltsjahr 2004/05 wurden weitere £58 Mio. zur Weiterführung der NDNAD zur Verfügung gestellt.¹⁰

6 Zu einem Überblick über die gesellschaftlichen Folgen des verbreiteten Einsatzes von Biometrie siehe Institute for Prospective Technological Studies 2005.

7 Schottland und Nordirland haben eigene Systeme, vgl. House of Lords. Select Committee on the Constitution 2009: vol. 1, S. 43. .

8 Vgl. die Auflistung der „Strategic objectives“ im Jahresbericht der NDNAD für das Jahr 2004-2005 (Home Office 2005)

9 Im internationalen Vergleich werden diese Hürden für die niedrigsten gehalten, vgl. Nuffield Council on Bioethics 2007: xxiv.

10 Alle Angaben nach Home Office (2005: 10).

Zu Beginn des zentralstaatlichen Finanzierungsprogramms hatte die Zielsetzung gelaute, bis März 2004 DNA-Proben aller „known active offenders“ in der Datenbank zu versammeln. Deren Zahl wurde auf zwischen 2,3 und 2,65 Mio. geschätzt (Home Office 2005: 10). Mittlerweile beträgt die Zahl der Einträge bald das Doppelte der damals geschätzten „aktiven Verbrecher“. Ob man sich aber in der ursprünglichen Schätzung geirrt hat oder es einfach sehr viele „newcomers to crime“ (ebd.) gibt, das wird in den offiziellen Dokumenten der britischen Regierung nicht thematisiert.

Zwischen 2000 und 2009 hat sich die Zahl der in der NDNAD gespeicherten Profile britischer Bürger nicht weniger als versechsfacht. Wie ungleich stärker der britische Staat damit seine Bürger überwacht, machen einige Vergleichszahlen deutlich: die im Verhältnis zur Bevölkerung zweitgrößte DNA-Datenbank – in Österreich – ist mit einem Prozent der Bevölkerung weniger als ein Siebtel so groß; und die nach Zahlen größte Datenbank – in den USA – erfasst in Relation zur Bevölkerung lediglich 0,5% und somit weniger als ein Vierzehntel des entsprechenden Wertes in Großbritannien (Nuffield Council on Bioethics 2007: 9).

Dabei sind die 7,4% im britischen Fall nur ein Durchschnittswert; für einzelne Bevölkerungsgruppen ist die Wahrscheinlichkeit, in der DNA-Datenbank erfasst zu sein weitaus größer. So ergeben Berechnungen aus Daten des britischen Innenministeriums, dass beinahe 40% der farbigen männlichen Bevölkerung in der Datenbank erfasst sind, während die entsprechenden Daten für asiatisch-stämmige Männer 13% und für weiße Männer 9% betragen.¹¹ Für Frauen ist sie entsprechend sehr viel geringer – sie dürfte im niedrigen einstelligen Prozentbereich liegen.

Über die Erfassten offenbart die Datenbank eine große Menge an sehr persönlicher Information. Oft wird ja von einem „DNA-Fingerabdruck“ (*DNA fingerprint*) gesprochen¹² und damit insinuiert, es handele sich bei dieser Methode lediglich um ein dem klassischen Fingerabdruck äquivalentes Verfahren. Doch dem ist nicht so: aus einem DNA-Profil kann weitaus mehr (und sehr viel persönlichere) Information abgelesen werden als aus einem Fingerabdruck,¹³ etwa Geschlecht, Verwandtschaftsbeziehungen und die Zugehörigkeit zu bestimmten ethnischen Gruppen ebenso wie Hinweise auf bestimmte Krankheiten. Welche zusätzlichen Erkenntnisse nach weiteren Fortschritten in den Analysetechniken in Zukunft noch aus den gegenwärtigen DNA-Profilen abzulesen sein werden ist nicht absehbar.

Die NDNAD ist die einzige DNA-Datenbank in Europa oder Nordamerika, die DNA-Profile auch aufbewahrt, wenn die betroffene Person freigesprochen wurde (Nuffield Council on Bioethics 2007: 52). Und da die NDNAD nicht durch eine einheitliche gesetzliche Grundlage, sondern durch einen Flickenteppich von Bestimmungen reguliert wird – bei dem die Polizei ein hohes Maß an Ermessensspiel-

11 Siehe den Bericht der BBC aus dem Jahr 2007 unter:
http://news.bbc.co.uk/2/hi/uk_news/6979138.stm [13.5.2009].

12 Vgl. z.B. den amerikanischen *DNA Fingerprint Act 2005*.

13 Vgl. zum Folgenden Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2007: 89).

raum hat und zudem das Verhältnis zum *Data Protection Act 1998* völlig unklar bleibt – muss die Situation unter dem Gesichtspunkt des Datenschutzes als besonders unbefriedigend angesehen werden.

1.3. Weitere Beispiele für Überwachung und Überwachungspläne in Großbritannien

Der umfassende Gebrauch von Kameras im öffentlichen Raum und die extensive Nutzung von DNA-Analyse und -Aufbewahrung sind nicht die einzigen Beispiele für die zu Beginn des Beitrags angesprochene Einschätzung des gegenwärtigen Großbritanniens als einer „Überwachungsgesellschaft“. Eine ganze Reihe weiterer staatlicher Vorhaben geht in dieselbe Richtung und rechtfertigt diese Bezeichnung zusätzlich. So baut die britische Polizei etwa unter dem (bereits an Orwell gemahnenden) Titel „Denying criminals the use of the road“ ein Programm zur automatisierten Überwachung des Straßenverkehrs auf. Dabei wird automatische Kennzeichenerkennung eingesetzt (*automatic number-plate recognition* oder ANPR), um die von strategisch platzierten Straßenkameras erfassten Autos in Echtzeit direkt mit verschiedenen nationalen Datenbanken abzugleichen. Dadurch können Verstöße gegen Führerscheinsperren oder Versäumnisse bei Zulassung, Versicherung, MOT¹⁴ oder Kfz-Versicherung direkt entdeckt und noch an der Straße geahndet werden (vgl. ACPO ANPR Steering Group 2005). Das System wird im Rahmen eines „National ANPR Data Centre“ so ausgebaut, dass im Jahr 2009 die Kapazität erreicht werden soll, pro Tag (!) 50 Mio. Kennzeichen von 10 Mio. Fahrern zu lesen. Diese Daten (die sich allein im Jahr 2009 auf 18 Mrd. Kennzeichensichtungen belaufen werden) sollen bis zu fünf Jahre gespeichert werden, ohne dass es dazu eines Vergehens bedürfte (Anderson 2009). Da es keine gesetzliche Regulierung für diesen Bereich gibt bleibt unklar, wofür diese Daten in Zukunft Verwendung finden werden.¹⁵ Auch die Grenzen werden elektronisch fortifiziert mithilfe des „e-Borders“-Programms, das seit 2004 existiert und dessen Zielsetzung vom britischen Innenministerium wie folgt beschrieben wird: „It will use on-line technology and advance passenger information provided by airlines before arrival to screen and record individuals as they enter and leave the UK, providing a comprehensive passenger movement audit trail.“¹⁶

Mittlerweile ist aus diesem Programm eine gigantische Datenbank geworden, die die jährlich 250 Mio. Ein- und Ausreisen aus Großbritannien speichert und dabei Namen, Adressen, Telefonnummern, Reisepläne und Kreditkartendetails aller Rei-

14 Entspricht dem deutschen TÜV.

15 Die Polizei setzt jedenfalls große Hoffnungen in das System, wie diese Zitat zum *National ANPR Data Centre* belegt: „This development forms the basis of a 24x7 vehicle movement database that will revolutionise arrest, intelligence and crime investigation opportunities on a national basis.“ (ACPO ANPR Steering Group 2005: 18)

16 Zitiert nach der Pressemitteilung des Home Office vom 28. September 2004: (<http://nds.coi.gov.uk/content/detail.asp?NewsAreaID=2&ReleaseID=130801>; [18.5.2009]). Für eine umfassendere Beschreibung siehe Amoore (2006).

senden für zehn Jahre aufbewahrt.¹⁷ Pläne für eine ähnlich umfassende Speicherung aller Kommunikationsdaten (Telefongespräche, SMS, Emails, aufgerufene Webseiten) in einer gigantischen Datenbank des Innenministeriums wurden seit Sommer 2008 diskutiert,¹⁸ im Frühjahr 2009 aber vorerst aufgegeben.¹⁹ Dabei dürften jedoch (trotz erheblicher Proteste, bis hin zum *Information Commissioner*) weniger plötzliche Bedenken hinsichtlich der Gefährdung der Privatsphäre eine Rolle gespielt haben, sondern die mit etwa 2 Mrd. Pfund erheblichen (und in der Wirtschaftskrise schwer zu rechtfertigenden) Kosten.²⁰

2. Warum so viel Überwachung?

Die im vorherigen Teil des Beitrages aufgeführten empirischen Beispiele machen deutlich, dass Großbritannien in vielen Bereichen der Überwachung verglichen mit anderen Ländern deutlich stärker engagiert ist und (sowohl nach eigener wie nach fremder Einschätzung) oft als weltweit am weitesten fortgeschritten zu betrachten ist. Die Privatsphäre des Bürgers ist hier vergleichsweise am weitesten zugunsten v.a. staatlicher Überwachung zurückgedrängt. Das erscheint erklärungsbedürftig, zumal angesichts der weitverbreiteten Vorstellung des Briten als eines ebendiese Privatsphäre besonders schätzenden und gegen Eindringlinge von außen verteidigenden Individuums („my home is my castle“).

Wie kann dieser Widerspruch zwischen Privatheitsliebe und Überwachungswirklichkeit erklärt werden? Im folgenden sollen dazu zwei Ansätze unternommen werden, von denen einer auf die spezifischen Charakteristika des Institutionensystems des britischen Staates abhebt, während der andere sich auf das Zusammenspiel von Nachfrage und Angebot im politischen Prozess konzentriert. Beide Ansätze verfolgen (im Sinne von *polity* und *politics*) unterschiedliche Perspektiven zur Erklärung von *policy*, doch schließen sie sich gegenseitig nicht aus. In der Tat wird gegen Ende des Beitrags argumentiert werden, dass die beste Erklärung für das hohe Ausmaß von Überwachung in der britischen Gegenwart wohl in einer Kombination beider liegt.

- 17 Vgl. die BBC-Meldung „Government plans travel database“ vom 8. Februar 2009 (http://news.bbc.co.uk/2/hi/uk_news/7877182.stm; [18.5.2009]).
- 18 Vgl. etwa die BBC-Meldungen „Warning over phone calls database“ vom 15. Juli 2008 (http://news.bbc.co.uk/1/hi/uk_politics/7507627.stm; [18.5.2009]) und „Hoon defends giant database plans“ vom 17. Oktober 2008 (http://news.bbc.co.uk/2/hi/uk_news/politics/7674775.stm; [18.5.2009]).
- 19 Vgl. „Jacqui Smith scraps plan for email database“ vom 27. April 2009 (<http://www.telegraph.co.uk/news/newstoppers/politics/5230123/Jacqui-Smith-scraps-plan-for-email-database.html>; [18.5.2009]).
- 20 Vgl. „Britische Regierung kippt zentrale Überwachungsdatenbank“ (<http://www.heise.de/newsticker/meldung/print/136877>; [13.5.2009]).

2.1. Die ungehinderte britische Mehrheitsdemokratie

Aus einer institutionell analysierenden Perspektive kann man die Stärke des britischen Überwachungsstaates als den Ausfluss eines Systems sehr weitgehend ungehinderter Regierungsmacht sehen, die ohne Rücksicht auf Gegenmächte und ohne die Einschränkung von formellen und informellen Kompromisszwängen agieren kann. In der Vergleichenden Politikwissenschaft wird dieses Syndrom unter den Stichworten „Mehrheitsdemokratie“ oder „Westminster-Demokratie“ behandelt.²¹ Dieses Modell eines politischen Systems ist – wie der Name schon besagt – mit dem britischen Demokratiemodell zwar nicht deckungsgleich, ihm aber doch sehr nahestehend. Es ist gekennzeichnet durch einen hochzentralisierten Staatsaufbau, in dem eine starke Einparteienregierung in ihrem Handeln nicht durch die Schutzmechanismen einer geschriebenen Verfassung behindert wird. Es gibt demzufolge keine relevanten „veto players“ (Tsebelis 2002), die der Regierung Kompromisse aufzwingen oder sie von ihrem geplanten Pfad abbringen können. Mechanismen, die dies in anderen Ländern (wie etwa der Bundesrepublik) bewirken können, existieren in Großbritannien nicht: es gibt dort weder einen Föderalismus, der andere Perspektiven als die des Zentralstaates in die politische Entscheidungsfindung einbringen könnte und / oder eventuell eine andere parteipolitische Mehrheit hat als die erste Parlamentskammer; zudem gibt es im Allgemeinen (und gab es tatsächlich seit Jahrzehnten) keine Koalitionsregierungen, deren Mitglieder sich auf Kompromisse einigen müssen, weil sie (aufgrund unterschiedlicher Anhängerschaften im politischen Spektrum) unterschiedliche politische Interessen in einer Frage verfolgen; und es gibt schließlich keine geschriebene Verfassung, die bestimmte politische Vorhaben als nicht mit der Verfassung vereinbar von vornherein verbietet oder – ein noch direkterer Eingriff in das politische Handeln der Regierung – durch ein Verfassungsgericht nach der Verabschiedung für verfassungswidrig erklärt. Eine Schutzinstanz jenseits der aktuellen politischen Mehrheit existiert in einem solchen System mithin nicht.

Ein Beispiel mag das illustrieren: Im März 2008 untersagte das Bundesverfassungsgericht in einem Urteil gegen entsprechende gesetzliche Bestimmungen in den Ländern Schleswig-Holstein und Hessen die Speicherung von durch automatische Kennzeichen-Erkennung gewonnenen Daten und erklärte, diese verletze das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitete Recht auf „informationelle Selbstbestimmung“.²² Zudem verletze die anlasslose Erfassung von Fahrzeugkennzeichen die Grundsätze der Normbestimmtheit und Verhältnismäßigkeit.²³ Dieses Kontrastbeispiel aus einem anderen politischen System macht deutlich, dass das

21 Vgl. zu Konzept und Empirie der Mehrheitsdemokratie klassisch Lijphart (1984) und Lijphart (1999).

22 Zu Entstehung und Wirkung des Grundrechts auf informationelle Selbstbestimmung siehe Busch/Jakobi (2009) (i.E.).

23 Urteil 1 BvR 2074/05 vom 11.3.2008 (http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html; [19.5.2009]).

weiter oben geschilderte Vorgehen der britischen Regierung im Bereich automatische Kennzeichenerkennung (ANPR) also nicht nur von politischem Willen, sondern auch von den Gegebenheiten des britischen Institutionensystems abhängig ist. Es ist dort deutlich einfacher, staatliche Kapazitäten für Überwachung durchzusetzen und in die Tat umzusetzen als dies in den meisten anderen politischen Systemen der Fall ist. Dies ist umso mehr der Fall, wenn eine Regierung (wie das bei der *New Labour*-Regierung seit 1997 der Fall war) sich die Nutzung von Synergieeffekten durch horizontale Integration von Verwaltungshandeln über verschiedene staatliche Handlungssphären hinweg unter dem Stichwort „joined-up government“ auf die Fahnen schreibt und daher das „sharing“ von Beständen personenbezogener Daten zu einem Politikziel erhebt – sowohl zu Zwecken von Kriminalitätsbekämpfung wie zur Verfolgung von Zielen sozialstaatlicher Intervention.²⁴ Überwachung entsteht dabei sowohl als geplante Haupt- wie als ungeplante Nebenwirkung der Politik.

2.2. New Labour-Wähler und New Labour-Politik

Neben einer auf institutionelle Zusammenhänge und die Plausibilität von Handlungslogiken abstellenden Analyse gibt es noch einen weiteren Ansatz, das im internationalen Vergleich sehr hohe Ausmaß an Überwachung im britischen Staat zu erklären. Dieser Ansatz läuft über die Mechanismen von politischem Angebot und politischer Nachfrage – also den Wünschen der Wählerschaft und den Politikangeboten politischer Parteien. Die deutliche Ausweitung von staatlicher Überwachung kann ja auch eine Reaktion auf (eventuell sich verändernde) Wünsche der britischen Wählerschaft sein, denen staatliche Politik nachkommt. Zwar ist die Vorstellung von den Briten als großen Anhängern bürgerlicher Freiheitsrechte verbreitet (s.o.), doch deuten neuere Erkenntnisse darauf hin, dass diese Vorstellung wohl nicht (mehr) der empirischen Realität entspricht. So lässt sich nach Auswertung der regelmäßig erhobenen Daten des „British Social Attitudes Survey“ schließen, dass eine Verschiebung weg von libertären Werten in diesem Bereich stattgefunden hat (Gearty/Johnson 2007). Obwohl es naheläge, eine Verschiebung der Präferenzen der britischen Wählerschaft in diesem Bereich mit den terroristischen Anschlägen vom 11. September 2001 in New York und Washington D.C. oder dem 7. Juli 2005 in London in Verbindung zu bringen, scheint der Meinungsumschwung davon unabhängig zu sein und hauptsächlich in der ersten Hälfte der 1990er Jahre stattgefunden zu haben (Gearty/Johnson 2007: 146).

Diese Verschiebung hinsichtlich abstrakter Rechte lässt sich auch anhand der Haltung zu konkreten Vorhaben nachvollziehen. Bei der Pflicht zum Führen eines Personalausweises (ein in Großbritannien umstrittenes Thema, das seit längerem heftig

24 Zum Ansatz des „joined-up government“ generell siehe Bogdanor (2005); zur speziellen Behandlung der Spannung zwischen Effizienzzielen und Datenschutz siehe (2005) und Belamy (2005). Zur generellen Strategie des *data sharing* siehe Cabinet Office 2005.

diskutiert wird) hat sich die Zahl der Gegner zwischen 1990 und 2005 von 40 auf 22 Prozent beinahe halbiert; und gleichzeitig ist die Zustimmung von 37 auf 54 Prozent gestiegen. Dabei hat sich die größte Veränderung bereits zwischen 1990 und 1994 ergeben, als sich binnen kurzer Zeit eine knappe Mehrheit *gegen* die Einführung solcher Ausweise in eine deutliche Zwei-Drittel-Mehrheit *für* die Einführung verwandelte (Gearty/Johnson 2007: 149). Dabei sind die Veränderungen in der Haltung zu Bürgerrechten nicht uniform verteilt: Sie sind am stärksten bei den Anhängern der *Labour Party* – die gemeinsam mit den *Liberal Democrats* traditionell als stärkste Unterstützer von Bürgerrechten galten (während die *Conservatives* sich gerne als Verteidiger von *law and order* präsentierten). Nimmt man die Unterstützung für das Recht auf Protestkundgebungen gegen die Regierung als Maßstab, so zeigt sich bei Anhängern der *Labour Party* ein besonders drastischer Rückgang: während bei ihnen die Unterstützung zwischen 1990 und 2005 um 27 Prozentpunkte *sinkt* (und bei den Liberaldemokraten um 14 Prozentpunkte), *steigt* sie bei den Anhängern der Konservativen um neun Prozentpunkte (Gearty/Johnson 2007: 153). Als Resultat ergibt sich eine deutliche Angleichung der Positionen der Parteianhänger (statt 23 Prozentpunkten Unterschied im Jahr 1990 beträgt dieser 2005 nur noch 14 Prozentpunkte) und es kommt zu einer Vertauschung von Positionen: Anhänger der Konservativen und der Liberaldemokraten liegen nun gleichauf in der Unterstützung der Bürgerrechte und liegen deutlich vor den Anhängern der Labour Party, die nun die geringste Unterstützung zeigen, während sie 1990 noch (beinahe) gleichauf mit den Liberaldemokraten lagen (ebd.).

Der im Hauptteil des Beitrages geschilderte Ausbau der Bürgerrechte einschränkende Überwachungspolitiken kann demnach als Reaktion der (seit 1997 regierenden) *New Labour*-Regierung auf die allgemein (und speziell unter ihren eigenen politischen Anhängern) gestiegene Nachfrage angesehen werden. Diese Perspektive hat den Vorteil, den Zeitpunkt des Ausbaus von Überwachungspolitik erklären zu können, was mit dem weiter oben geschilderten institutionellen Ansatz nicht gelingt. Die beiden Ansätze sind allerdings insoweit gut miteinander kombinierbar, als dass die politischen Absichten der Labour-Regierung hinsichtlich des Ausbaus von Überwachung dank des institutionellen Rahmens besonder leicht und ohne Widerstände im britischen politischen System umsetzbar waren. Und obwohl die Terroranschläge der Jahre 2001 und 2005 nicht ursächlich für den Umschwung in der Haltung waren, beförderten sie den von der Regierung Blair eingeschlagenen (und später unter Premierminister Gordon Brown ab 2007 fortgesetzten) Kurs der hinsichtlich der Bürgerrechte immer restriktiveren Politik, da die führenden Politiker von *New Labour* alle Pläne zur Einführung neuer oder Verschärfung existierender Überwachungspolitiken mit Verweis auf die terroristische Gefahr begründen konnten und davon auch reichlich Gebrauch machten²⁵ – denn, so zeigen Analysen, die

25 Vgl. den Schwerpunkt auf und die große Zahl der Gesetzesvorhaben im Bereich „Innere Sicherheit“ für das Wahljahr 2005 in der BBC-Meldung „Crime fight tops Labour's agenda“ vom 23.11.2004

Beschreibung einer Maßnahme als zur Bekämpfung des Terrorismus gedacht erhöht deren Akzeptanz auch dann, wenn der genaue Zusammenhang unklar bleibt (Garty/Johnson 2007: 169). Die Notwendigkeit der Einführung einer (schließlich stor- nierten, s.o.) Datenbank, in der alle Kommunikationsdaten gespeichert werden soll- ten, wurde etwa von Innenministerin Smith mit den Worten begründet, diese sei „vital to fighting terrorism and combating serious crime, including child sex abuse, murder and drugs trafficking.“²⁶ Und Verkehrsminister Hoon drückte wahrschein- lich das generelle Grundrechtsverständnis der *New Labour*-Regierung aus als er formulierte: „The biggest civil liberty of all is not to be killed by a terrorist.“²⁷

3. Schluss

Zum Abschluss des Beitrags soll noch einmal auf George Orwell und sein Buch über den totalen Überwachungsstaat zurückgekommen werden. Die Hauptfigur des Romans, Winston Smith, endet als gebrochener Mann:

„Er blickte hinauf zu dem riesigen Gesicht. Vierzig Jahre hatte er gebraucht, um zu erfassen, was für ein Lächeln sich unter dem dunklen Schnurrbart verbarg. [...] Zwei nach Gin duftende Tränen rannen an den Seiten seiner Nase herab. Aber nun war es gut, war alles gut, der Kampf beendet. Er hatte den Sieg über sich selbst errungen. Er liebte den Großen Bruder“ (Orwell 2000: 273).

Doch dass Smith so endet, ist nicht das Resultat von Überwachung – es ist das Re- sultat von Folter. Und daher ist auch völlig klar, dass die Parallelen zwischen dem orwell'schen Überwachungsstaat und dem gegenwärtigen britischen Staat deutliche Grenzen haben. Denn wie kritisch auch eine Bestandaufnahme der politischen Kurs- entscheidungen in Fragen von Überwachung und Privatheit ausfallen mag, so steht es doch außer Frage, dass Großbritannien ein Rechtsstaat ohne totalitäre Tendenzen ist.

Aber es bedarf keiner totalitären Tendenzen, um die getroffenen Entscheidungen und die Entwicklung hin zu einem Überwachungsstaat bedenklich zu finden und in ihr erhebliche Gefahren für die Freiheitsrechte der einzelnen Bürger zu sehen. Denn der weiter oben in diesem Beitrag deutlich gewordene Wunsch des britischen Staa- tes, vorbeugende Sicherheit durch das Sammeln immer detaillierterer Daten über immer mehr Bürger zu erreichen gefährdet die bürgerlichen Freiheiten in mehrfa- cher Hinsicht. Da ist zum einen die Gefahr, dass die so gesammelten Daten in frem- de Hände gelangen, durch Unachtsamkeit und Inkompetenz der staatlichen Stellen.

(http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/4034543.stm, [22.5.2009]). Siehe auch (in vergleichender Perspektive) Haubrich (2003) und Lyon (2003).

26 Vgl. die BBC-Meldung „Giant database plan 'Orwellian'“ vom 15.10.2008

(http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm, [22.5.2009]).

27 Vgl. die BBC-Meldung „Hoon defends giant database plans“ vom 17.10.2009

(http://news.bbc.co.uk/2/hi/uk_news/politics/7674775.stm, [22.5.2009]).

Großbritannien ist in dieser Hinsicht ein besonders gefährliches Pflaster, denn die Zahl der Vorfälle in diesem Bereich scheint hier besonders hoch zu sein, ebenso wie ihre Ernsthaftigkeit.²⁸ Zum anderen besteht die Gefahr, dass gesammelte Daten auch innerhalb des Staates neue Begehrlichkeiten wecken und für andere als ursprünglich vorgesehene Zwecke Verwendung finden – was v.a. wegen des relativ schwachen Datenschutzregimes Grund zur Sorge bietet. Und schließlich und grundsätzlich ist zu befürchten, dass sich der britische Staat in einen „Präventionsstaat“ verwandelt, der rechtsstaatliche Grundsätze wie Verhältnismäßigkeit, Unschuldsvermutung und Zweckgebundenheit zugunsten von Sicherheitsmaximierung, vorbeugendem Handeln und instrumenteller Effizienz vernachlässigt.²⁹

Regan (1990: 50) führte – wie weiter oben ausgeführt – vor beinahe zwanzig Jahren die spezifische Art der Institutionalisierung im Bereich Datenschutz auf die Schwäche des britischen Staates zurück, der zwischen den miteinander konkurrierenden Verfassungskonventionen der Parlamentsouveränität und der ministeriellen Verantwortlichkeit gefangen war und so keine wirklich unabhängige Kontrolle von Datenschutz durchsetzen konnte. Derselbe Staat erweist sich im Bereich der Nutzung und des Ausbaus von Überwachungstechniken zu Zwecken der Inneren Sicherheit als ausgesprochen stark, weil durch konstitutionelle und politische Faktoren mehr oder weniger völlig unbehindert. Gleichzeitig bleiben aber Elemente von Schwäche erkennbar, die sich etwa in der Unkoordiniertheit des Handelns zeigen – so im Bereich der Ausstattung der CCTV-Systeme, wo enorme Geldsummen ausgegeben wurden ohne Gedanken auf Fragen von Standardisierung zu verschwenden und als Ergebnis enorme Defizite bei Interoperabilität, Speicherbarkeit und übergreifender Nutzbarkeit bestehen.³⁰

Die schon erwähnten Probleme bei Datenverlusten fordern den britischen Staat nun heraus und haben das Thema auf der politischen Tagesordnung weit nach oben gebracht. Nachdem mehrere Berichte von Stiftungen und Verbänden das Thema forciert hatten, haben auch die beiden Kammern des britischen Parlaments Untersuchungskommissionen eingesetzt, die umfangreiche Berichte vorgelegt und Empfehlungen ausgesprochen haben.³¹ Ob diese Empfehlungen Gehör bei der Regierung

28 Siehe dazu die Liste von Datenverlusten auf der website des britischen *Information Commissioner's Office* (http://www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf; [24.5.2009]), den Untersuchungsbericht von Poynter 2008 oder die website <http://ukliberty.wordpress.com/data-loss/> (24.5.2009).

29 Zum Konzept des Präventionsstaates siehe Denninger (1990), Denninger (2002) und Prantl (2007).

30 „The contribution CCTV has made in protecting the public and assisting the police to investigate crime has occurred despite CCTV systems being developed in a piecemeal fashion with little strategic direction, control or regulation. This approach has failed to maximise the potential of our CCTV infrastructure and many involved in its operation and management felt there remained a pressing need to examine existing standards, procedures, training and methods of operation.“ (Gerrard 2007: 5)

31 Zu den angesprochenen Berichten gehören Surveillance Studies Network 2006, Royal Academy of Engineering 2007, Nuffield Council on Bioethics 2007 und Crossman 2007; die Par-

finden, bleibt abzuwarten – die bei Abschluss des Manuskripts gerade veröffentlichte Stellungnahme der Regierung zu den Empfehlungen im Bericht des House of Lords (United Kingdom Government 2009) weckt keine allzu großen Erwartungen in dieser Richtung. Andererseits kann man spekulieren, dass ein Wechsel in der Regierung zumindest potentiell eine substantielle Wandlung der politischen Dynamik in diesem Politikfeld herbeiführen könnte – vielleicht durch eine konservative Regierung, die (eventuell im Verbund mit den Liberaldemokraten) den Schutz der Bürgerrechte auf ihre Fahnen schreibt; und nach einigen Jahren in der Opposition könnte dann vielleicht auch die Labour Party ihre traditionelle Neigung für eine bürgerrechtsfreundliche Position in diesem Bereich wieder entdecken.

Literatur

- 6, Perri/Raab, Charles/ Bellamy, Christine 2005: Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I, in: Public Administration 83, S. 111–133.
- ACPO ANPR Steering Group 2005: ANPR Strategy for the Police Service 2005/2008. Denying Criminals the Use of the Roads, in:
http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc;
 [18.05.2009].
- Amoore, Louise 2006: Expert report: Borders, in: Surveillance Studies Network (Hrsg.): A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network, in:
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.
- Anderson, Ross/Brown, Ian/Dowty, Terri/Inglesant, Philip/Heath, William/ Sasse, Angela 2009: Database state. A report commissioned by the Joseph Rowntree Reform Trust Ltd, York.
- Audit Commission 1993: Helping with enquiries. Tackling crime effectively, London.
- Bellamy, Christine/6, Perri/ Raab, Charles 2005: Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II, in: Public Administration 83, S. 393–415.
- Bennett, Colin J. 1992: Regulating privacy. Data protection and public policy in Europe and the United States, Ithaca.
- Bogdanor, Vernon (Hrsg.) 2005: Joined-up government, Oxford.
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit 2007: Tätigkeitsbericht 2005–2006. 21. Tätigkeitsbericht, Berlin.
- Busch, Andreas/ Jakobi, Tobias 2009: Die Erfindung eines neuen Grundrechts. Zu Konzept und Auswirkungen der „informationellen Selbstbestimmung“, in: Hönnige, Christoph (Hrsg.). Verfassungswandel im Mehrebenensystem, Wiesbaden, i.E..

lamentsberichte sind House of Commons. Home Affairs Committee 2008 und House of Lords. Select Committee on the Constitution 2009.

- Cabinet Office* 2005: Transformational government. Enabled by technology. November 2005, London.
- Crossman, Gareth* 2007: Overlooked – Surveillance and personal privacy in modern Britain, in: <http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf>, [13.05.2009].
- Denninger, Erhard* 1990: Der Präventions-Staat, in: Denninger, Erhard (Hrsg.): Der gebändigte Leviathan, Baden-Baden, S. 33–49.
- Denninger, Erhard* 2002: Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz, in: Aus Politik und Zeitgeschichte, S. 22–30.
- Flaherty, David H.* 1989: Protecting privacy in surveillance societies. The Federal Republic of Germany, Sweden, France, Canada, and the United States, Chapel Hill/London.
- Gearty, Conor/ Johnson, Mark* 2007: Civil liberties and the challenge of terrorism, in: Parker, Alison (Hrsg.): British Social Attitudes: the 23rd Report. Perspectives on a changing society, London, S. 143–182.
- Gerrard, Graeme/Parkins, Garry/Cunningham, Ian/Jones, Wayne/Hill, Samantha/ Douglas, Sarah* 2007: National CCTV Strategy, London.
- Gill, Martin/Spriggs, Angela/Allen, Jenna/Argomaniz, Javier/Bryan, Jane/Jessiman, Patricia/Kara, Deena/Kilworth, Jonathan/Little, Ross/Swain, Daniel/ Waples, Sam* 2005: The impact of CCTV. Fourteen case studies. Home Office Online Report 15/05, London.
- Goold, Benjamin J.* 2004: CCTV and policing. Public area surveillance and police practices in Britain, Oxford.
- Haubrich, Dirk* 2003: September 11, anti-terror laws and civil liberties. Britain, France and Germany compared, in: Government and Opposition 38, S. 3–28.
- Home Office* 2005: The National DNA Database Annual Report 2004–2005, in: http://www.homeoffice.gov.uk/documents/NDNAD_AR_04_051.pdf, [08.05.2009].
- House of Commons. Home Affairs Committee* (Hrsg.) 2008: A Surveillance Society? Fifth Report of Session 2007–08, London.
- House of Lords. Select Committee on the Constitution* (Hrsg.) 2009: Surveillance: Citizens and the State. 2nd Report of Session 2008–09, London.
- Information Commissioner's Office* 2007: Annual Report 2006/07, London.
- Institute for Prospective Technological Studies* 2005: Biometrics at the Frontiers. Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). Brüssel.
- Interpol DNA Unit* 2003: Global DNA Database Inquiry. Results and Analysis, in: <http://www.interpol.int/Public/Forensic/dna/Inquiry/InquiryPublic2002.pdf>, [13.05.2009].
- Kammerer, Dietmar* 2008: Bilder der Überwachung, Frankfurt am Main.
- Lijphart, Arend* 1984: Democracies. Patterns of majoritarian and consensus government in twenty-one countries, New Haven.
- Lijphart, Arend* 1999: Patterns of democracy. Government forms and performance in thirty-six countries, New Haven, Conn.
- Lyon, David*, 2003: Surveillance after September 11, Malden (MA).
- Lyon, David* 2007: Surveillance studies. An overview, Cambridge.
- McCahill, Michael/ Norris, Clive* 2002: CCTV in Britain. Urbaneye Project Working Paper No. 3, Hull.
- Norris, Clive/ Armstrong, Gary* 1999: The maximum surveillance society. The rise of CCTV, Oxford.

- Nuffield Council on Bioethics* 2007: The forensic use of bioinformation. Ethical issues, London.
- Orwell, George* 2000: 1984. Übersetzung von Kurt Wagneseil, München.
- Poynter, Kieran* 2008: Review of information security at HM Revenue and Customs. Final report, London.
- Prantl, Heribert*: Der grosse Rüssel. Jeder Bürger wird zum Ausländer im eigenen Land: Vom Umbau des Rechtsstaats in einen Präventionsstaat, in: *Süddeutsche Zeitung*, 21.04.2007, S. 15.
- Privacy International* 2007: The 2007 International Privacy Ranking, in:
<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597;>
 [05.05.2009].
- Raab, Charles D.* 1993: Data Protection in Britain. Governance and Learning, in: *Governance* 6, S. 43–66.
- Regan, Priscilla M.* 1990: Protecting Privacy and Controlling Bureaucracies. Constraints of British Constitutional Principles, in: *Governance* 3, S. 33–54.
- Royal Academy of Engineering* 2007: Dilemmas of privacy and surveillance. Challenges of technological change, London.
- Schröder, Detlef* 2007: Videoüberwachung in Großbritannien und den USA, in: Bücking, Hans-Jörg (Hrsg.): *Polizeiliche Videoüberwachung öffentlicher Räume*, Berlin, S. 41–51.
- Surveillance Studies Network* 2006: A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network.
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.
- Tsebelis, George* 2002: *Veto players. How political institutions work*, New York/Princeton.
- United Kingdom Government* 2009: The Government Response to the House of Lords Select Committee on the Constitution's Report *Surveillance: Citizens and the State*. Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty. 13 May 2009.
- Williams, Chris A.* 2003: Police Surveillance and the Emergence of CCTV in the 1960s, in: *Gill, Martin* (Hrsg.): *CCTV*, Leicester, S. 9–21.

