Erster Teil

Grundlagen

I. Einleitung

A. Auf dem Weg ins digitale Panopticon?

Im Jahr 1787 veröffentlichte der englische Jurist und Sozialphilosoph Jeremy Bentham den Bauplan für eine neuartige Strafanstalt – das sogenannte *Panopticon*.[1] In diesem Modellgefängnis sollte eine umfassende Disziplinierung der Häftlinge primär durch dessen besondere Architektur erreicht werden. Grundgedanke des *Panopticons* ist es, alle Insassen einer Anstalt von einer zentralen Position aus beaufsichtigen zu können. Bentham konstruierte ein kreisförmiges, mehrstöckiges Gebäude, in dessen Mittelpunkt ein Beobachtungsturm steht, von dem aus die am Rand jeder Ebene angebrachten Zelltrakte strahlenförmig abgehen. Da die Räume völlig voneinander isoliert sind und in jedem nur eine Person untergebracht wird, ist es den Häftlingen unmöglich, die Mitgefangenen zu sehen, sie zu hören und mit ihnen zu kommunizieren. Der Wärter in der Mitte des Gebäudes hingegen kann die einzelnen Zellen beobachten, ohne dass die Insassen ihn wahrnehmen können. Dies ist möglich, weil die Gefangenen im künstlichen Gegenlicht permanent dessen Blicken ausgesetzt sind, er selbst aber im Dunkel des Beobachtungsturms unsichtbar bleibt. Folglich wissen die Häftlinge nicht, ob sie gerade tatsächlich beobachtet werden oder nicht.[2] Im Ergebnis soll auf diesem Weg mit geringem personellem Aufwand eine große Zahl von Menschen unter Kontrolle gehalten werden können.

Als charakteristisch für das *Panopticon* erweist sich die Annahme Benthams, dass durch die Möglichkeit der ständigen Überwachung Willfährigkeit bei den Insassen erzeugt werden könne, ohne den Häftlingen gegenüber physischen Zwang anwenden zu müssen. Diesen Grundgedanken des *Panopticons* griff in den 70er Jahren des 20. Jahrhunderts der fran-

1 Vgl Bentham, Panopticon Writings (Neuauflage 2011); Božovič (Hrsg), Jeremy Bentham – The Panopticon Writings (1995) 31 ff.

2 Vgl Niesen, Macht der Publizität. Jeremy Benthams Panoptismen, in: Krause/Rölli (Hrsg), Macht – Begriff und Wirkung in der politischen Philosophie der Gegenwart (2008) 221 (223).

zösische Philosoph und Historiker Michel Foucault in seinem Werk *Überwachen und Strafen*[3] auf, in dem er die Entwicklung moderner Strafsysteme untersuchte und die Auswirkung ständiger Kontrolle auf die Überwachten analysierte. Maßgeblich am *Panopticon* sei, so Foucault, dass die Gefangenen nicht wirklich permanent von den Wärtern beobachtet werden, sie dies subjektiv aber so empfinden. Das *Panopticon* sei somit gleichsam eine Art Theater, in dem die Illusion ständiger Überwachung aufgeführt wird.[4] Diese Vorstellung bleibt für ihre Protagonisten nicht ohne Folge. Foucault beschreibt die Wirkung auf die Überwachten wie folgt: *„Derjenige, welcher der Sichtbarkeit unterworfen ist und dies weiß, übernimmt die Zwangsmittel der Macht und spielt sie gegen sich selber aus; er internalisiert das Machtverhältnis, in dem er gleichzeitig beide Rollen spielt; er wird zum Prinzip der eigenen Unterwerfung."*[5] Anders formuliert: Die Insassen beginnen sich selbst zu beaufsichtigen. Im Bewusstsein der permanent möglichen Überwachung kontrollieren sie laufend ihr eigenes Verhalten und passen schlussendlich auch ihr Denken der Kontrolle an.[6]

Die von Bentham verfassten Pläne – die er nicht nur auf Haftanstalten angewendet wissen wollte, sondern auch auf Krankenhäuser, Kasernen, Schulen und Fabriken – wurden (auch wenn sie Einfluss auf die spätere Architektur von Gefängnissen hatten[7]) nie verwirklicht, weder zu seinen Lebzeiten noch danach.[8] Als Metapher für die Gefahren der modernen Informationsgesellschaft hat das *Panopticon* aber überlebt und erfährt in der aktuellen Debatte zum Datenschutz eine Renaissance. Quer durch die wissenschaftlichen Disziplinen wird heute untersucht, welche Auswirkungen die ausufernde Sammlung und Speicherung personenbezogener Daten, ihre zunehmend multifunktionale Verwendung und die systematische Vernetzung privater wie öffentlicher Datenbanken auf das Verhalten der Menschen hat – wobei mahnend auf Benthams Pläne Bezug genommen wird.[9] Der Begriff vom *„digitalen Panoptikum"* wurde

3 Foucault, Surveiller et punir: La naissance da la prison (1975); Dt: Überwachen und Strafen – Die Geburt des Gefängnisses (1976).

4 Vgl Whitaker, Das Ende der Privatheit (1999) 47.

5 Foucault, Überwachen und Strafen, 260.

6 Vgl de Swaadf, Die Totale Überwachung, Spiegel-Online, 6.12.2006, abrufbar unter: http://www.spiegel.de/wissenschaft/mensch/0,1518,452041,00.html [Stand: April 2014]

7 Zum Einfluss der Ideen Benthams auf die Architektur – insbesondere von Haftanstalten – siehe Nutz, Strafanstalt als Besserungsmaschine (2001) 176ff, 181ff; Barton/Barton, Modes of Power in Technical and Professional Visuals, JBTC 1993, 138; Semple, Bentham's prison: a study of the panopticon penitentiary (1993).

8 Das einzige Projekt zum Bau eines Gefängnisses nach den Plänen Benthams wurde 1811 abgebrochen. Bentham wurde für seinen Aufwand zwei Jahre später mit dem Betrag von £ 23.000 entschädigt.

9 So etwa Rössler, Der Wert des Privaten (2001) 219; Whitaker, Privatheit 46 f; Simon/Simon, Ausgespäht und abgespeichert (2008) 33; Bürdek (Hrsg), Der digitale

zum verbreiteten Synonym für jene fortschreitenden technischen Entwicklungen, die eine Bedrohung der Privatsphäre der Bürger befürchten lassen.[10]

Der Vergleich der digitalen Informationsgesellschaft des 21. Jahrhunderts mit dem Modell eines aus der Sicht des 18. Jahrhunderts „idealen" Gefängnisses mag übertrieben erscheinen. Im Gegensatz zu den Gefängnisinsassen in Benthams Haftanstalt ist die Handlungsfreiheit des Bürgers heute zweifelsohne nicht per se durch staatlichen Zwang beschränkt. Zu fragen ist aber, ob der Effekt der Selbstregulierung des Bürgers infolge tatsächlicher oder auch nur vermeintlicher Überwachung und Informationskontrolle, den Foucault als die charakteristische Wirkungsweise des *Panopticons* ansah, nicht auch in der heutigen Welt allgegenwärtiger elektronischer Datenverwendung wirksam wird.

Nun ist es an sich kein neues Phänomen, dass staatliche Stellen – aber auch Private – Informationen über Bürger sammeln. Der technische Fortschritt der letzten Jahrzehnte hat aber dazu geführt, dass die Möglichkeiten zur Datensammlung eine neue Qualität erreicht haben. Das Netz der Informationskontrolle, das über die Bürger gespannt ist, wird infolge des stetig steigenden Einsatzes von Informationstechnologien mit jedem Jahr engmaschiger. Dies lässt sich anhand einiger Entwicklungen veranschaulichen: Im Jahr 2000 wurde davon ausgegangen, dass zu jeder Österreicherin und jedem Österreicher rund 400 Datensätze in privaten und öffentlichen Datenverarbeitungen gespeichert waren.[11] Für das Jahr 2014 lässt sich diese Zahl kaum mehr seriös berechnen.[12] Datenschützer gehen aber – abhängig vom Alter, den Lebensgewohnheiten und der soziographischen Positionierung der Person – von durchschnittlich 500 bis 2.000 Datensätzen pro Bürger aus. In Bezug auf technikaffine und in diesem Sinn „datenexponierte" Menschen kann sich dieser Wert auf bis zu 5.000 Datensätze erhöhen, die in öffentlichen oder privaten Datenanwendungen verwendet werden. In Österreichs Städten überwachen derzeit geschätzte

Wahn (2001) 178 ff; Solove, The digital person: technology and privacy in the information age (2006) 98; Nagenborg, Das Private unter den Rahmenbedingungen der IuK-Technologie (2005) 148; Lyon, Theorizing surveillance: the panopticon and beyond (2006) 9; Levin/Frohne/Weibel, CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother (2002).

10 So weist die Internetsuchmaschine Google zum Begriff *„digital panopticon"* 13.900 Treffer aus [Stand April 2014].

11 Peissl/Cas, Beeinträchtigung der Privatsphäre in Österreich (2000) 11; Zeger/Widerin/Kronegger, Erfahrungen zum Datenschutz 1980 – 1998 (1999) 42.

12 Zur Qualität und zur Eingriffstiefe verwendeter Daten siehe Sterbik-Lamina/Peissl/Cas, Privatsphäre 2.0 – Beeinträchtigung der Privatsphäre in Österreich, ITA-Projektbericht (2009).

250.000 Videokameras rund 30.000 Standorte.[13] Jede bargeldlose Zahlung und Finanztransaktion, die wir vornehmen, wird und bleibt heute gespeichert – und dies nachweislich nicht nur vom zuständigen Kreditinstitut.[14] Kein Telefonat wird mehr geführt, kein E-Mail verschickt und keine Website angeklickt, ohne dass dieser Vorgang nicht registriert wird. Bei jeder Nutzung des Internets wird eine Datenspur hinterlassen, die über Tätigkeiten, Interessen und Vorlieben Auskunft gibt.[15] Selbst die Tatsache, wo sich eine Person gerade aufhält, kann – sofern sie ein Mobiltelefon bei sich hat – im städtischen Bereich auf bis zu fünf Meter genau bestimmt werden.[16]

Vor diesem Hintergrund stellt sich die Frage, ob und inwieweit unsere Handlungsfreiheit vom stetig wachsenden Einsatz von Informationstechnologien unberührt bleiben kann. Müssen wir davon ausgehen, dass wir – im Bewusstsein dessen, dass ein Großteil unseres täglichen Verhaltens beobachtet oder aufgezeichnet wird – unser Sozial-, Kommunikations- und Konsumverhalten zwangsläufig anpassen? Können wir unsere Individualität weiterhin frei ausleben und die eigene Persönlichkeit selbstbestimmt entfalten, auch wenn wir wissen, dass unsere Handlungen infolge umfassender elektronischer Datenverarbeitungen nicht mehr dem Vergessen anheim fallen können?[17] Oder haben wir uns damit abzufinden, dass in der digitalen Welt im Sinn Benthams und der Analyse Foucaults die gesamte Gesellschaft einer permanenten Sichtbarkeit unterworfen ist, der sich der Einzelne nicht mehr entziehen kann?

13 Zeger, Mensch. Nummer. Datensatz (2008) 188.

14 Vgl Hattenberger, Recht auf Privatsphäre. Rechtliche, insbesondere datenschutzrechtliche Überlegungen vor dem Hintergrund wachsender Informationsbedürfnisse, in: Greif/Mitrea/Werner (Hrsg), Information und Gesellschaft – Technologien einer sozialen Beziehung (2008) 99 (100).

15 Siehe dazu beispielhaft Trojanow/Zeh, Angriff auf die Freiheit (2009); Becker, Datenschatten – Auf dem Weg in die Überwachungsgesellschaft? (2010); Reischl, Die Google-Falle: Die unkontrollierte Weltmacht im Internet (2008); Staudinger, Wo Internet-User ihre Spuren hinterlassen, in: Jaksch-Ratajczak (Hrsg), Aktuelle Fragen der Internetnutzung (2010) 233.

16 Von dieser Möglichkeit haben die österreichischen Sicherheitsbehörden im Jahr 2008 in 695 Fällen, im Jahr 2009 in 776 Fällen, im Jahr 2010 in 913 Fällen und im Jahr 2012 in 1.081 Fällen Gebrauch gemacht, ohne dass die betroffenen Bürger von den einschreitenden Stellen hiervon in Kenntnis gesetzt werden mussten. Vgl Anfragebeantwortung der BMI vom 24.11.2008, XXIII. GP-NR, 4954/AB zur Anfrage der Abg. Maier und Genossen vom 24.9.2008, 5008/J; Anfragebeantwortung der BMI vom 23.6.2008, XXIII. GP, 4148/AB zur Anfrage des Abg. Zach und weiterer Abgeordneten vom 23.4.2008, 4130/J; Burgstaller/Pühringer, Aktuelles vom Rechtsschutzbeauftragten, SIAK-Journal 2013/3, 14.

17 Vgl Mayer-Schönberger, Nützliches Vergessen, in: Reiter/Wittmann-Tiwald (Hrsg), Goodbye Privacy – Grundrechte in der digitalen Welt (2008) 9; ders, Delete – Die Tugend des Vergessens in digitalen Zeiten (2010).

B. Untersuchungsgegenstand und Aufbau der Arbeit

Angesichts der aufgeworfenen Fragen untersucht die vorliegende Arbeit, inwieweit die österreichische Rechtsordnung den Bürgern jenen Freiraum vor informationeller Kontrolle einräumt, der für die freie Entfaltung der Persönlichkeit erforderlich ist. Dargestellt wird – mit einem Focus auf verfassungs- und verwaltungsrechtliche Bestimmungen – zum einen, welche Grenzen das heimische Recht der elektronischen Datenermittlung und -verwendung ohne Einwilligung des Betroffenen setzt. Zum anderen wird erörtert, welcher Rechtsschutz dem Einzelnen offensteht, wenn er sich dagegen zur Wehr setzen will, dass Behörden und/oder Private Kenntnis von nicht allgemein zugänglichen Aspekten seiner Person und seines Lebens erlangen und diese Angaben computerunterstützt speichern und nutzen. In Abgrenzung dazu wird aber auch der Frage nachgegangen, in welchen Bereichen und unter welchen rechtlichen Rahmenbedingungen automationsunterstützte Datenverwendungen auch ohne Zustimmung des Betroffenen für rechtlich zulässig erklärt werden. In welchen Konstellationen geht die Rechtsordnung davon aus, dass das Interesse der Allgemeinheit oder jenes eines Privaten derart gewichtig ist, dass es gegenüber dem Anspruch auf informationelle Selbstbestimmung des Betroffenen überwiegt?

Den Ausgangspunkt der Arbeit bildet zunächst eine grobe Skizzierung jener technischen Entwicklungen, die dazu geführt haben, dass der Begriff der Privatheit in der Literatur kaum mehr verwendet wird, ohne nicht gleichzeitig auf seine Bedrohung hinzuweisen oder sein nahes Ende in Aussicht zu stellen.[18] Die umfassende Möglichkeit der Digitalisierung und Vernetzung von Daten sowie die Miniaturisierung der Informations- und Kommunikationstechnologie haben aus technischer Sicht neue Rahmenbedingungen geschaffen, unter denen der rechtliche Schutz der Privatsphäre nunmehr betrachtet werden muss.

Daran anschließend werden im zweiten Teil der Arbeit jene Grundrechte erörtert, aus denen sich ein verfassungsrechtlicher Schutz der informationellen Privatsphäre in Bezug auf die elektronische Datenverarbeitung ergibt. Untersucht werden – nach einem kurzen Überblick über die historische Entwicklung der Privatsphäre und ihres rechtlichen Schut-

---

18 So beispielsweise Peissl (Hrsg), Privacy – Ein Grundrecht mit Ablaufdatum? (2003); Tichy/Peissl, Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, in: Österreichische Juristenkommission (Hrsg), Grundrechte in der Informationsgesellschaft (2001) 22; Whitaker, Das Ende der Privatheit (1999); Schaar, Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft (2007); Etzioni, The Limits of Privacy (1999); Schulzki-Haddouti (Hrsg), Vom Ende der Anonymität[2] (2001); Heller, Post Privacy: Prima leben ohne Privatsphäre (2011).

zes – die dafür maßgeblichen grundrechtlichen Gewährleistungen der österreichischen Verfassungsrechtsordnung, nämlich das Grundrecht auf Achtung des Privatlebens, das Grundrecht auf Datenschutz, das Fernmeldegeheimnis sowie damit verbunden das Recht auf Achtung der Korrespondenz. Auf eine Darstellung jener Grundrechte, die zwar ebenfalls Aspekte der Privatheit zum Gegenstand haben, in Bezug auf den Schutz vor den besonderen Gefahren der elektronischen Datenverarbeitung aber keine praktische Bedeutung besitzen – das Hausrecht einerseits sowie das Briefgeheimnis andererseits –, wird hingegen verzichtet. Daran anschließend wird der unionsrechtliche Grundrechtsschutz mit Privatsphärenbezug behandelt. Das abschließende Kapitel des zweiten Teils untersucht zum einen, wie die Verhältnismäßigkeit von Grundrechtseingriffen zu beurteilen ist, die in Form der Ermittlung und Verwendung von Informationen erfolgen, zum anderen wird erörtert, wie in Bezug auf solche Informationseingriffe ein wirksamer Rechtsschutz auszugestalten ist.

Gegenstand des dritten Teils der Arbeit sind die rechtlichen Rahmenbedingungen, die das DSG 2000 – als für Datenverwendungen im Allgemeinen maßgebliche gesetzliche Grundlage – für die Verarbeitung personenbezogener Daten aufstellt. Im Vordergrund stehen dabei jene materiellen Bestimmungen, mit denen die berechtigten Geheimhaltungsinteressen der Betroffenen geschützt werden. Im Konkreten wird untersucht, unter welchen Voraussetzungen das Verwenden und Übermitteln personenbezogener Daten zulässig ist und welche Pflichten das Gesetz dem Auftraggeber zum Schutz der Vertraulichkeit und Sicherheit der Datenverarbeitung auferlegt. Darüber hinaus wird dargestellt, welche Rechte den Betroffenen gegenüber dem Auftraggeber eingeräumt werden und welche Rechtsbehelfe ihnen dafür offenstehen.

Die Schlussbetrachtungen im vierten Teil der Arbeit widmen sich schließlich den möglichen Strategien für eine Modernisierung des Datenschutzrechts. Erörtert wird, inwieweit die bestehenden datenschutzrechtlichen Instrumentarien adaptiert werden sollten und welche neuen Schutzmechanismen erforderlich wären, um die Privatheit der Bürger auch im 21. Jahrhundert wirksam schützen zu können.

II. Entwicklungslinien in der Informations- und Kommunikationstechnologie

Die technischen Entwicklungen der vergangenen Jahrzehnte und die damit einhergehende Durchdringung nahezu aller Lebensbereiche mit

Informations- und Kommunikationstechnologien haben das Alltagsleben der Menschen und die Arbeitswelten unserer Gesellschaft grundlegend verändert.[19] Neben den unbestrittenen Annehmlichkeiten, die die neuen Technologien wie etwa das Internet und die mobile Telekommunikation mit sich bringen, bergen diese aber auch Gefahren für die Privatsphäre der Bürger. Dass ihnen ein beträchtliches Kontroll- und Missbrauchspotential innewohnt, gehört mittlerweile weitgehend zum Allgemeinbewusstsein.[20] Nicht grundlos wird in der Literatur vom *„Janusgesicht der Informationsgesellschaft"* gesprochen.[21] In gleichem Maße, wie sich nämlich die Anwendungsbereiche der Informations- und Kommunikationstechnologien laufend weiterentwickelt haben, haben sich Umfang und Dichte der dabei anfallenden Daten über ihre Nutzer erhöht und damit Möglichkeiten der Informationskontrolle stetig erweitert.

Aus technischer Sicht waren es drei sich gegenseitig bedingende Entwicklungen, die die Voraussetzungen für die breite Nutzung der Informations- und Kommunikationstechnologien und ihre Anwendung in immer weiteren Bereichen unseres Alltags geschaffen haben: die Digitalisierung der Daten, die Miniaturisierung der Technologie und die Vernetzung der Datenanwendungen.[22] Alle drei Aspekte haben zum einen die Nutzungsmöglichkeiten und die Verbreitung der Informations- und Kommunikationstechnologie maßgeblich beeinflusst und zum anderen die Auswirkungen ihrer Verwendung auf die Privatsphäre der Bürger geprägt.

A. Digitalisierung

Der Begriff Digitalisierung bezeichnet in seinem Kern die Umwandlung der zur Darstellung von Informationen und Signalen verwendeten elektronischen Analoggrößen in Digitalsignale, also die Überführung kontinuierlicher Größen in diskrete, dh zeitlich oder räumlich getrennte Wer-

19 Dazu grundlegend Castells, Das Informationszeitalter: Wirtschaft, Gesellschaft, Kultur, 3 Bde (2004); Palfrey/Gasser, Born digital – Understanding the First Generation of Digital Natives (2008); Steinbicker, Zur Theorie der Informationsgesellschaft[2] (2011); Mattelart, Kleine Geschichte der Informationsgesellschaft (2003).

20 Siehe Peissl, Privacy in Österreich: Eine Bestandsaufnahme, in: Peissl, (Hrsg), Privacy – Ein Grundrecht mit Ablaufdatum? (2003) 155; Hattenberger, Privatsphäre 99, die pointiert formuliert, dass *„es ein Allgemeinplatz [ist], dass in der Informationsgesellschaft die Privatsphäre besonderen Gefährdungen ausgesetzt ist"*.

21 Tichy/Peissl, Privatsphäre 22.

22 Waneckel, Persönlichkeitsschutz in der Informationsgesellschaft (1999) 43; Tichy/Peissl, Privatsphäre 22 f; Peissl, Prinzipien des Datenschutzes und ihre Verwirklichung im medizinischen Bereich, in: Stelzer (Hrsg), Biomedizin – Herausforderung für den Datenschutz (2005) 1 (8).