Arbeiterkammer Wien

constitutional
thinking
beyond
borders

Priv.-Doz. Dr.
Konrad Lachmayer
Meldemannstraße 18/1.03
1200 Vienna // Austria
+43 676 5665992
konrad@lachmayer.eu
www.lachmayer.eu

Demokratierechtliche Analyse der Entwicklungsperspektiven des Datenschutzrechts

Priv.-Doz. Dr. Konrad Lachmayer

Inhaltsverzeichnis

5. Zusammenfassung und Ausblick

Bibliografie

Autor der rechtswissenschaftlichen Analyse

Priv.-Doz. Dr. Konrad Lachmayer

Dr. Konrad Lachmayer ist selbstständiger Wissenschafter in Wien. Er lehrt als Privatdozent am Institut für Staats- und Verwaltungsrecht der Universität Wien und forscht als Akademischer Rat am Institut für Rechtswissenschaften der ungarischen Akademie der Wissenschaften. Forschungsschwerpunkte bestehen im Europäischen Verwaltungsverbund, im Internationalen und Vergleichenden Verfassungsrecht sowie im Datenschutz und Polizeirecht.

Dr. Lachmayer studierte Rechtswissenschaft an der Universität Wien und verbrachte Forschungsaufenthalte an der University of Cambridge, dem Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht in Heidelberg, an der Central European University in Budapest sowie am Europakolleg Hamburg. Im Jahr 2010 wurde Konrad Lachmayer die Venia aus Verfassungsrecht, Verwaltungsrecht und Europarecht verliehen.

Kontakt: konrad@lachmayer.eu; www.lachmayer.eu

Demokratierechtliche Analyse der Entwicklungsperspektiven des Datenschutzrechts

Konrad Lachmayer

1. Einleitung

A. Entwicklungen des österreichischen und europäischen Datenschutzrechts

Auf den ersten Blick wirkt das österreichische Datenschutzrecht sehr staatlich.[1] Aufgrund staatlicher Gesetzgebung regulieren staatliche Behörden, wie die unabhängige Datenschutzbehörde, das Datenschutzrecht. Es bestehen staatliche Datenschutzregister und eine Meldepflicht des Auftraggebers. Das Datenschutzrecht befindet sich allerdings im Umbruch und die genannten Elemente des Datenschutzrechts werden sich in naher Zukunft stark verändern.

Das nationale Datenschutzrecht, das bereits jetzt durch die europäische Datenschutzrichtlinie geprägt ist,[2] soll durch unmittelbar anwendbares Europarecht substituiert werden.[3] Geplant ist eine Datenschutz-Grundverordnung, die im Entwurf der Kommission aus 2012 (in weiterer Folge: Entwurf) sowie in einer durch das Europäische Parlament adaptierten Fassung

[1] Siehe zu den Grundlinien des DSG *Lehner,* Das Datenschutzgesetz 2000, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 121.

[2] Siehe *Westphal*, Grundlagen und Bausteine des europäischen Datenschutzrechts, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 53.

[3] *Lachmayer*, Zur Reform des Europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, Österreichische Juristenzeitung 2012, 841.

vorliegt. Diese Datenschutz-GrundVO wird die bisherige DatenschutzRL ersetzen und zu massiven Änderungen im europäischen wie nationalen Datenschutzrecht führen. Es ist geplant, das innerstaatliche Datenschutzregister durch Datenschutzbeauftragte in Unternehmen zu ersetzen, womit die Meldepflicht von Datenschutzanwendungen entfällt. Die Datenschutzbehörde soll stärkere Strafkompetenzen erhalten und die Bedeutung von privaten Zertifizierungen wird im Datenschutzrecht erheblich zunehmen.[4]

Dieser Umbruch im Datenschutzrecht steht unter fraglichen Vorzeichen der Effektivität des Datenschutzrechts insgesamt.[5] Insbesondere stehen global tätig Konzerne im Vordergrund, deren AGBs (als eine Form der Rechtssetzung Privater) mittels Zustimmung eine breite und oft unüberschaubare Datenverwendung ermöglichen. Die Versuche der Beschränkung derartigen Ausuferns von Datenverwendungen waren bisher nur begrenzt mit Erfolg gekrönt (siehe etwa die Bemühung von *europe* versus *facebook*).[6] Hervorhebenswert ist aber das richtungsweisende Urteil des EuGH in Hinblick auf ein Recht auf Vergessen in Hinblick auf Suchmaschinen (am Anlassfall *Google*).[7]

Längst lässt sich die Rechtssetzung durch Private im Datenschutzrecht nicht mehr nur auf globale Konzerne reduzieren. Die Verwendung personenbezogener Daten hat aus unterschiedlichsten Gründen in vielfältiger Weise in allen Wirtschaftszweigen Einzug gehalten. Damit gemeint sind ganz unterschiedliche Geschäftsmodelle von Videoüberwachungen in Einkaufszentren über Kundenbindungs- und -analysestrategien durch Kundenrabatte auf Kundenkarten

[4] Ebenda.
[5] Siehe *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, ÖJT GA I/1 (2012) 50ff.
[6] http://www.europe-v-facebook.org/DE/de.html.
[7] Siehe EuGH, 13.5.2014, Google Spain und Google, Rs C-131/12.

bis hin zu datensammelnde *smartphone-apps* von *start-up* Unternehmen.[8] Die datenschutzrechtliche Problemsituation bleibt dieselbe: Kunden stellen ihre Daten Unternehmen zur Verfügung, ohne dass sie – abgesehen von einer Pauschal-Zustimmung – die Möglichkeit hätten, ihre datenschutzrechtlichen Präferenzen zu präzisieren.

Es soll daher der Forschungsfrage nachgegangen werden, inwieweit im Rahmen der zunehmenden Privatisierung datenschutzrechtlicher Regelbildung demokratische Grundsätze Berücksichtigung finden bzw. welche Kritikpunkte aus den Perspektiven von Partizipation, Repräsentation, Legitimation, Verantwortung und Transparenz bestehen.

B. Demokratische Dimensionen des Datenschutzrechts

Dem Datenschutzrecht kommt in besonderer Weise eine transnationale Dimension zu, da die Datenverwendung in Zeiten informationeller Globalisierung nicht an nationalstaatlichen Grenzen endet. Damit wird es der typischerweise nationalstaatlich organisierten Demokratie erschwert, entsprechende Regelungen zur Verfügung zu stellen. Aus diesem Blickwinkel erscheint eine Europäisierung des Datenschutzrechts nur konsequent, um im Rahmen der demokratischen Verfahren in der Europäischen Union[9] datenschutzrechtliche Regelungen zu erlassen. Die Verwendung personenbezogener Daten lässt sich aber nicht auf die EU beschränken, sondern ist in ihrer globalen Dimension zu verstehen. Insoweit hängt im Datenschutzrecht viel von der Effektivität der Regelungen außerhalb Europas ab: man denke an die Versuche von europäischer Ebene aus Übereinkünfte mit den Vereinigten Staaten zu treffen, etwa in Form der Safe

[8] *Lachmayer*, Datenschutzrecht als Öffentliches Wirtschaftsrecht, in: Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 13 (2013) 9 (16ff).
[9] Siehe *von Bogdandy*, Grundprinzipien, in ders/Bast (Hrsg), Europäisches Verfassungsrecht² (2009) 13 (62).

Harbour Regelungen.[10] An einem Vollstreckungsübereinkommen mit den USA im Datenschutzbereich fehlt es allerdings[11] und es ist zumindest fragwürdig, inwieweit durch Safe Harbour der Umsetzung der europäischen Datenschutzbestimmungen in den Vereinigten Staaten zum Durchbruch verholfen wird.[12] Im Bereich der Kommunikation, der IT-Dienstleistungen und des Informationsaustausches ist die Wirtschaft als globalisiert zu verstehen und es greift zu kurz, nur die internationale Kooperation mit den USA zu betrachten. Insoweit ergeben sich im Bereich des Outsourcing etwa nach Indien (, das ein demokratisch organisiertes Land ist,) und in Bezug auf die Vertragsbeziehungen, die durch das Internet in alle Welt entstehen, noch viel größere demokratierechtliche Fragestellungen bei der Festlegung von datenschutzrechtlichen Regelungen.[13]

Versteht man das Datenschutzrecht in seiner Dimension als Wirtschaftsrecht[14], so stellt sich die Frage der staatlichen Determinierung privater datenschutzrechtlicher Verwendung. ArbeitnehmerInnen und KonsumentInnen sind insbesondere abhängig, die ihnen in Form von AGBs[15] oder Musterverträgen zur Verfügung gestellten datenschutzrechtlichen Bedingungen anzunehmen. Demokratische Legitimation liegt hier an der Offenheit des Verfahrens, an den Rechtsschutzmöglichkeiten des Einzelnen und an den staatlichen Rahmenbedingungen zur inhaltlichen Ausgestaltung.

---

[10] Siehe näher zu den Safe Harbour Bestimmungen *Kuner*, European Data Protection Law: Corporate Compliance and Regulation (2007) Rz 4.59.

[11] Im Juni 2014 gab es Absichtserklärungen der US Administration den Datenschutz für europäische BürgerInnen zu verbessern; siehe http://derstandard.at/2000002307478/Datenschutz-USA-ueberlegen-Beschwerderecht-fuer-EU-Buerger.

[12] Siehe etwa *Hötzendorfer/Schweighofer*, Safe Harbour in der „Post-Snowden-Ära", in Lück-Schneider ua (Hrsg), Gemeinsam Electronic Government ziel(gruppen)gerecht gestalten und organisieren (2014) 125.

[13] Siehe einen globalen Überblick über nationales Datenschutzrecht *Lee Bygrave*, Data Privacy Law. An International Perspective (2014) 99.

[14] *Lachmayer*, Datenschutzrecht als Öffentliches Wirtschaftsrecht, in: Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 13 (2013) 9.

[15] Siehe zur Problematik Radin, *Boilerplate* (2013).

In Hinblick auf die darüber hinausgehende Auslagerung datenschutzrechtlicher Kontrolle, ist auch die Legitimation der Akteure und die Effektivität der Kontrolle und damit letztlich die Verantwortlichkeit der relevanten Akteure angesprochen. Soweit die Konkretisierung inhaltlicher Vorgaben des Datenschutzrechts durch private Regelbildung erfolgt, besteht ebenso die Frage nach der Legitimation der regelbildenden Akteure und der Transparenz des damit verbundenen Verfahrens.

Die demokratischen Dimensionen des Datenschutzrechts gestalten sich daher als vielfältig und sind im Rahmen demokratierechtlicher Analysekriterien näher zu untersuchen.

C. Demokratierechtliche Analysekriterien

Eine Überprüfung anhand demokratierechtlicher Maßstäbe muss an der österreichischen Verfassung ansetzen. Private Rechtssetzer sind nicht am Maßstab eines Gesetzgebers (direkte Wahl, Parteiensystem, detailliertes Gesetzgebungsverfahren etc.) zu messen,[16] sondern an jenen verfassungsrechtlichen Vorgaben, die typischerweise für die demokratische Legitimation der Verwaltung herangezogen werden.[17] Dies erscheint insoweit adäquat, als auch die Verwaltung generell in Form von Verordnungen gesetzeskonkretisierend tätig wird. Als Elemente einer demokratischen Legitimation kommen daher primär personelle und inhaltliche Kriterien[18] in Betracht.

---

[16] Siehe dazu *Öhlinger/Eberhard*, Verfassungsrecht[10] (2014) Rz 342.

[17] dazu etwa *Grabenwarter*, Die demokratische Legitimation weisungsfreier Kollegialbehörden in der staatlichen Verwaltung. Zur Zulässigkeit der Entsendung von Organwaltern durch nicht demokratisch legitimierte Einrichtungen, in Haller ua (Hrsg) Staat und Recht. FS Winkler (1997) 271 (282ff).

[18] Ebenda.

Als personelle demokratische Legitimation werden jene Elemente angesehen, die sich auf die Legitimation der involvierten Akteure beziehen. Dabei stehen Bestellung, Zeitdauer im Amt und Abbestellung (Verantwortlichkeit) im Vordergrund.[19] Über die personelle Komponente der Legitimation hinaus spielen Fragen der inhaltlichen Legitimation eine Rolle. Diese kann entweder durch die Weisungsbindung in einem hierarchischen System[20] erreicht werden, wenn die Weisungsbefugten in besonderer Weise einer demokratischen Legitimation oder Kontrolle unterliegen,[21] oder aber etwa durch Aufsichtsmodelle.[22] Die inhaltliche Legitimation wird auch durch Gesetzesbindung iSd Art 18 B-VG vermittelt.[23]

Neben den starken Elementen der demokratischen Legitimation kann Legitimation in Verfahren auch durch Transparenz, öffentliche Diskussion und Partizipation verstärkt werden.[24] Schließlich kann neben den input-orientierten Legitimationsaspekten auch auf output-orientierte Legitimation (unabhängige Sachentscheidung, Sachverstand, Rationalität, Effizienz etc.)[25] geachtet werden.[26]

Ausgehend von diesen verfassungsrechtlichen Vorgaben sollen die Akteure, die Verfahren und das Rechtsinstrumentarium im Bereich des Datenschutzrechts auf ihre demokratierechtlichen Dimensionen hin analysiert werden (siehe sogleich unter 2.). Über die an der Erstellung beteiligten Akteure hinaus werden auch die

---

[19] Ausgangspunkt sind die verfassungsrechtlichen Konzepte zur BReg und den BM gem Art 69 ff B-VG.

[20] So Art 20 Abs 1 B-VG.

[21] Siehe *Raschauer*, Art 20 Abs 1 B-VG, in Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht. Kommentar 3. Lfg (2000) Rz 6.

[22] Siehe Art 20 Abs 2 B-VG. Siehe aber auch zur Selbstverwaltung Art 115ff, Art 120a B-VG. Siehe dazu *Hauer*, Aufsicht und Kontrolle, in ÖVG (Hrsg), Selbstverwaltung in Österreich (2009) 75.

[23] Zur demokratischen Seite des Legalitätsprinzips siehe *Rill*, Art 18 B-VG, in Kneihs/Lienbacher (Hrsg), Rill-Schäffer-Kommentar. Bundesverfassungsrecht 1. Lfg. (2001) Rz 1ff.

[24] Siehe dazu *von Bogdandy*, Grundprinzipien, in ders/Bast (Hrsg), Europäisches Verfassungsrecht² (2009) 13 (66).

[25] Siehe die Elemente in Art 20 Abs 2 B-VG.

[26] Siehe *Grabenwarter/Holoubek*, Demokratie, Rechtsstaat und Kollegialbehörden mit richterlichem Einschlag. Zu den verfassungsrechtlichen Grenzen der Einrichtung von Kollegialbehörden nach Art 20 Abs 2 und Art 133 Z 4 B-VG, ZfV 2000, 194.

Verfahren zur Erstellung bzw. Änderung datenschutzrechtlicher Regelungen untersucht (siehe unter 3.). Schließlich werden auch unterschiedliche datenschutzrechtliche Regelungsinstrumente in Hinblick auf demokratierechtlich relevante Elemente hin überprüft (siehe 4.). Insgesamt liegt das Augenmerk auf den sich verändernden Bedingungen im Datenschutzrecht.

2. Akteure

A. Von der Datenschutzkommission zur Datenschutzbehörde

In den letzten fünf Jahren hat sich die staatliche Organisation des Datenschutzrechts wesentlich gewandelt. Im Jahr 2010 agierte als zentrale Behörde des Datenschutzrechts die beim Bundeskanzleramt eingerichtete Datenschutzkommission. Der Rechtsschutz gegen die Bescheide der DSK ging an die Gerichtshöfe des öffentlichen Rechts.[27]

Die Änderungen in der Organisation der Datenschutzbehörde hängen zum einen mit einem Urteil des EuGH zur Unabhängigkeit der Datenschutzkommission und zum anderen mit der Einführung der Verwaltungsgerichtsbarkeit erster Instanz zusammen.[28] Der EuGH hielt in seinem Urteil vom 16.10.2012, Rs C-614/10, Kommission/Österreich, fest, dass die Unabhängigkeit der Datenschutzkommission nicht ausreichend ausgestaltet ist. Die Eingliederung im Bundeskanzleramt verstieß ebenso wie die Dienstaufsicht gegen die DatenschutzRL.[29]

Die neu ausgestaltete Datenschutzbehörde ist monokratisch und nicht mehr kollegial organisiert. Damit ist ein Element deliberativer Entscheidungsfindung verloren gegangen, das weder von Seiten der EU kritisiert noch aufgrund der Schaffung der Verwaltungsgerichtsbarkeit geboten war. Die vom EuGH gebotene Unabhängigkeit hat rechtsstaatlich unzweifelhafte Vorteile, womit aber die

---

[27] *Kimm*, Rechtsschutz im Datenschutz, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 153.

[28] Siehe die DSG-Novelle 2014, BGBl I 2013/83.

[29] Siehe *Bresich/Riedl/Souhrada-Kirchmayer*, Die völlig unabhängige Datenschutzkontrollstelle, ZfRV 2014, 52 (55ff).

Möglichkeiten demokratischer Legitimation verringert wurden. Die Stärkung der neu eingerichteten Datenschutzbehörde gegenüber privater Rechtssetzung hängt aber auch an der personellen und finanziellen Ausstattung.

Bereits die Datenschutzkommission ebenso wie die mit 2014 neu eingerichtete Datenschutzbehörde sind im internationalen Vergleich mit geringen Ressourcen ausgestattet.[30] Es fehlt damit an der notwendigen Anzahl an MitarbeiterInnen, primär im technischen aber auch im juristischen Bereich, um eine adäquate Kontrolle der stetig wachsenden Informationsverarbeitungen von Unternehmen durchzuführen. Um eine effektive Kontrolle durch die Datenschutzbehörde zu ermöglichen, müssen die institutionellen Rahmenbedingungen zur Verfügung gestellt werden. Nur auf diese Weise ist die Einhaltung der gesetzlichen Rahmenbedingungen in Form einer staatlichen Kontrolle möglich.

Ein noch bestehendes Problem der Datenschutzbehörde liegt in der mangelnden Durchführung von Verwaltungsstrafverfahren durch die Datenschutzbehörde, da diese bisher bei den Bezirksverwaltungsbehörden (BVB) durchgeführt wurden. Diesbezüglich verstärkt sich das schon genannte personelle Problem nochmals. Die BVB können im Vergleich zur spezialisierten Datenschutzbehörde noch viel weniger das nötige rechtliche und technische Know-How für die Durchführung der Verwaltungsstrafen zur Verfügung stellen. Die Ausstattung der Datenschutzbehörde mit der Kompetenz, Verwaltungsstrafen zu verhängen, wie sie im Entwurf zur DatenschutzVO vorgesehen sind, stärkt die Möglichkeiten der staatlichen Kontrolle.

---

[30] Siehe aber die gegenteiligen Aussagen der Leiterin der Datenschutzbehörde: http://oe1.orf.at/artikel/378256; zurzeit 24 MitarbeiterInnen, davon 12 Akademiker (https://www.bka.gv.at/site/7878/default.aspx); siehe zum internationalen Vergleich http://futurezone.at/netzpolitik/oesterreich-vor-datenschutz-scherbenhaufen/62.275.980.

Die zunehmende Unabhängigkeit der Datenschutzbehörde und die damit verbundene Agentifizierung der Organisation des Datenschutzrechts[31] wird durch die geplante EU-Datenschutzverordnung noch weiter an Bedeutung gewinnen. Die staatliche Kontrolle über Unternehmen könnte durch Stärkung der staatlichen Strukturen gelingen, hängt aber von der Ausgestaltung der Kompetenzen derselben ab.

Die zukünftige Weiterentwicklung der Datenschutzbehörde hängt zentral von der Erlassung der europäischen Grund-VO ab. So sieht der Entwurf der Grund-VO neben der Überwachung und Gewährleistung der GrundVO auch die Möglichkeit zur Erlassung von Verwaltungsstrafen vor.[32]

B. Der Datenschutzbeauftragte

Nach dem bestehenden Konzept werden Datenanwendungen der Datenschutzbehörde gem § 17 DSG gemeldet. Ausnahmen bestehen im Rahmen von Standardanwendungen, deren Verwendung durch die Standard- und MusterVO meldefrei gestellt ist.[33] Durch das Datenschutzregister wird den Datenanwendungen ein Publizitätscharakter verliehen und überdies der Datenschutzbehörde im Rahmen ihrer Kontrollmöglichkeiten ein Instrumentarium in die Hand gegeben, um die bestehenden Datenanwendungen zu überprüfen. Zentrale Problematik des Registers und der Kontrolle ist die Effektivität in Hinblick auf die personelle Ausstattung der Datenschutzbehörde.[34]

---

[31] Damit gemeint ist die zunehmende Umwandlung der staatlichen Behörde in eine Struktur, die einer EU-Agentur ähnelt. Siehe zum Phänomen *Müller*, „Agentur hat Konjunktur" – „Agencification" und demokratische Verwaltungslegitimation", JBÖffR 2011, 261.

[32] *Souhrada-Kirchmayer*, Der Entwurf eines neuen Datenschutz-Rechtsrahmens der Europäischen Union, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 2012 (2012) 9 (12,23).

[33] *Navacchi*, Die Registrierung von Datenanwendungen, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 195 (198ff).; *Jahnel*, Handbuch Datenschutzrecht (2010) 324ff; *Kotschy*, Die Änderungen im Registrierungsverfahren nach der DSG-Novelle 2010, in N. Raschauer (Hrsg), Datenschutzrecht 2010 (2011) 51.

[34] http://futurezone.at/netzpolitik/oesterreich-vor-datenschutz-scherbenhaufen/62.275.980.

Das Meldemodell des Datenverarbeitungsregisters wird in einem engen Anwendungsbereich (etwa bei der Verwendung sensibler Daten oder bei Verwendung von Daten in Hinblick auf die Kreditwürdigkeit von Menschen) durch ein Bewilligungsmodell ergänzt (Vorabkontrolle gem § 18 Abs 2 DSG). Die Effektivität des Bewilligungsmodells hat sich punktuell – wie etwa bei *Google Street View* – bestätigt.[35]

Das Konzept der Registrierung erscheint allerdings bereits als ein Modell mit Ablaufcharakter. Die staatliche Erfassung der Datenanwendungen soll durch ein Modell der sog. Datenschutzbeauftragten ersetzt werden. Ziel ist es, die als bürokratisch eingestufte Meldepflicht durch unternehmensinterne Strukturen zu ersetzen. Bemerkenswerterweise sind die Bemühungen, ein derartiges Modell auf nationaler Ebene vor Erlassung der europäischen Datenschutz-GrundVO einzuführen, gescheitert.[36] Dieses Modell hätte es den Unternehmen ermöglicht, durch die Bestellung eines Datenschutzbeauftragten und Nennung des Namens desselben an die Datenschutzbehörde aus der Meldepflicht entlassen zu werden.

Das Modell der EU-DatenschutzgrundVO geht an dieser Stelle noch weiter. Der Entwurf zur GrundVO[37] sieht keine Registrierung durch die Datenschutzbehörde mehr vor, stattdessen wird fix ein Datenschutzbeauftragter vorgesehen – allerdings nur bei Unternehmen mit mehr als 250 MitarbeiterInnen oder in dem Fall, dass die Kerntätigkeit des Unternehmens in der regelmäßigen und systematischen Beobachtung von Menschen liegt (Art 35 Entwurf). Der unternehmensinterne Datenschutzbeauftragte muss über entsprechendes Fachwissen verfügen, darf keine anderen Interessenskonflikte haben und muss

[35] Siehe https://www.dsb.gv.at/site/6733/default.aspx.
[36] Siehe dazu den Ministerialentwurf zu einer DSG-Novelle 2012, 397/ME.
[37] Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endg; siehe dazu *Lachmayer*, Zur Reform des Europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, ÖJZ 2012, 841.

zumindest für zwei Jahre bestellt werden; er kann sowohl intern (innerhalb des Unternehmens) als auch extern (außerhalb der Unternehmensstruktur) organisiert sein. Der Datenschutzbeauftragte ist in seiner Funktion unabhängig und ist vom Unternehmen in den Datenschutz betreffende Fragen einzubinden und mit den notwendigen Ressourcen auszustatten. Die Aufgabenfelder sind denkbar breit konzipiert und beziehen sich nicht nur auf Unterrichts-, Beratungs- und Dokumentationspflichten, sondern auch auf die Überwachung der Umsetzung der Datenschutzverordnung sowie weiterer Überwachungsaufgaben.[38]

Der Datenschutzbeauftragte wird in einem Unternehmen zum zentralen Akteur um datenschutzrechtliche Belange umzusetzen. Während sich die Datenschutzbehörde auf (stichprobenartige) Kontrollen und Rechtsschutzverfahren beschränkt, liegt es nun am Datenschutzbeauftragten, die Umsetzung des Datenschutzrechts im Unternehmen zu gewährleisten. Die Problematik des Datenschutzbeauftragten liegt in der zentralisierten Zuständigkeit bei gleichzeitiger Abhängigkeit von der Unternehmensleitung sowohl in Hinblick auf seine eigene Person als auch in Hinblick auf die Umsetzung datenschutzrechtlicher Vorgaben. Die zweijährige Bestelldauer schafft ebenfalls keine ausreichende Unabhängigkeit.

Das Europäische Parlament hat in diesem Sinne unterschiedliche Änderungen des Entwurfs zur GrundVO vorgeschlagen. Der Ansatz mit 250 Mitarbeitern erscheint zu hoch gegriffen und erfasst die datenschutzrechtliche Problematik nicht adäquat. Der Entwurf des Europäischen Parlaments sieht vielmehr als Grenze für die Einführung eines Datenschutzbeauftragten die Verarbeitung von 5.000 Betroffenen vor. Insgesamt bleibt die Problematik eines äquivalenten Schutzes für Unternehmen mit weniger Mitarbeitern bzw. Datensätzen bestehen. Das

[38] Siehe Art. 37 Entwurf.

Europäische Parlament schlägt bei internen Mitarbeitern eine vierjährige Zuständigkeit eines Datenschutzbeauftragten vor. Der Parlamentsentwurf betont die Funktion des Datenschutzbeauftragten als Bewusstseinsbilder für Datenschutz im Unternehmen, nimmt aber gleichzeitig die Geschäftsführung (Vorstand) des Unternehmens in die Pflicht, die datenschutzrechtlichen Maßnahmen umzusetzen.

Aus demokratischer Sicht geht durch die Einführung des Datenschutzbeauftragten die primäre staatliche Kontrolle verloren und wird nur zum Teil durch einen datenschutzrechtlichen Beauftragten ersetzt. Der partielle Rückzug des Staates auf Rechtsschutz-, stichprobenartige Kontroll- und Strafverfahren ist in Hinblick auf die stetig wachsende Bedeutung des Datenschutzes als problematisch zu bewerten. Die Substitution durch einen Datenschutzbeauftragten überzeugt nur zum Teil. Wenn es gelingt, durch einen Datenschutzbeauftragten eine Informationsdrehscheibe für Datenschutz in den Unternehmen anzusiedeln, so ist in Hinblick auf das Datenschutzbewusstsein und die Einhaltung von Datenschutzbestimmungen etwas gewonnen. Verbleibt der Datenschutzbeauftragte in der Abhängigkeit der an ökonomischen Kriterien orientierten Geschäftsführung, so kann dieser leicht – unter den in Diskussion befindlichen Organisationsstrukturen – zum Feigenblatt reduziert werden. Durch den Datenschutzbeauftragten geht jedenfalls die Öffentlichkeitsfunktion des Datenschutzregisters und damit ein wesentliches demokratisches Element des Datenschutzrechts verloren. Überdies steht der Datenschutzbeauftragte nicht in einer stärkeren Kooperationsbeziehung mit der Datenschutzbehörde, womit es der Kontrolle der Kontrolleure ebenso ermangelt wie eines Informationsflusses von Datenschutzbeauftragten zur Datenschutzbehörde. Mit dem inner-unternehmerischen Datenschutzbeauftragten wird die regulatorische Kontrolle des Datenschutzrechtes entstaatlicht und damit die demokratische Legitimation entscheidend reduziert.

C. Europäische Akteure

- Einleitung

Das Datenschutzrecht hat auf die informationellen Realitäten Rücksicht zu nehmen und ist daher in seiner transnationalen Dimension zu begreifen. Umso wichtiger werden die transnationalen bzw. europäischen Akteure, die es erst ermöglichen, Fragen des Datenschutzrechts – zumindest in Europa – adäquat zu adressieren. Mit der Einführung einer für ganz Europa geltenden Datenschutz-GrundVO wird ein einheitlicher europäischer Datenschutzstandard geschaffen, der über die bestehende DatenschutzRL hinausgeht.[39] Als zentrale Akteure jenseits des Mitgliedsstaates sind zu allererst die jeweils anderen datenschutzrechtlichen Aufsichtsbehörden zu identifizieren, sodann der Europäische Datenschutzausschuss, die Europäische Kommission sowie der Europäische Datenschutzbeauftragte. Für die Rechtssetzung durch Private spielen die europäischen Akteure in unterschiedlicher Weise eine Rolle. Zu erwähnen sind etwa die Regelungen zum anwendbaren Recht in Hinblick auf die Niederlassung eines Unternehmens bzw. die damit verbundene Zuständigkeit der relevanten Kontrollstellen (Aufsichtsbehörden). Am Beispiel von Facebook wird klar ersichtlich, dass der jeweiligen räumlichen Zuständigkeit eine signifikante Bedeutung zukommt. Der EuGH hat dieses Konzept jüngst relativiert.[40] Umso

[39] Siehe bisher zur Datenschutzrichtlinie *Westphal*, Grundlagen und Bausteine des europäischen Datenschutzrechts, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 53.

[40] EuGH 13.05.2014, Rs C-131/12, Google Spain / Agencia Española de Protección de Datos. "Zum räumlichen Anwendungsbereich der Richtlinie führt der Gerichtshof aus, dass es sich bei Google Spain um eine Tochtergesellschaft von Google Inc. in Spanien und somit eine „Niederlassung" im Sinne der Richtlinie handelt. Das Argument, die von Google Search vorgenommene Verarbeitung personenbezogener Daten werde nicht im Rahmen der Tätigkeiten dieser Niederlassung in Spanien ausgeführt, weist er mit folgender Begründung zurück: „Bei der Verarbeitung personenbezogener Daten zum Betrieb einer Suchmaschine durch ein Unternehmen mit Sitz in einem Drittstaat, das aber in einem Mitgliedsstaat eine Niederlassung besitzt, wird die Verarbeitung im Sinne der Richtlinie „im Rahmen der Tätigkeiten" dieser Niederlassung ausgeführt,

bedeutender wird aber die Koordination der unterschiedlichen mitgliedsstaatlichen Aufsichtsbehörden. Die Rolle der Europäischen Kommission ist etwa im Zusammenhang mit Drittstatten und der Übermittlung personenbezogener Daten hervorzuheben. Die geplante Datenschutz-GrundVO sieht jedenfalls eine Stärkung der transnationalen Akteure vor.

- Das Zusammenwirken der Datenschutzbehörden in Europa

Die datenschutzrechtlichen Kontrollstellen/Aufsichtsbehörden sind nicht nur unabhängig, sondern stehen auch im Wettbewerb miteinander. Umso wichtiger ist die Zusammenarbeit und Koordination zwischen den Kontrollstellen. Durch die geplante Datenschutz-GrundVO soll die Zusammenarbeit wesentlich ausgebaut werden. Über die Amtshilfe (Art 55 Entwurf) sind gemeinsame Maßnahmen der Aufsichtsbehörden gem Art 56 Entwurf vorgesehen, von denen mehrere Mitgliedsstaaten betroffen sind. Überdies ist ein Kohärenzverfahren inklusive Dringlichkeitsverfahren vorgesehen. Das Kohärenzverfahren soll vor allem zur Anwendung kommen, wenn der freie Verkehr von personenbezogenen Daten beeinträchtig wird, oder wenn etwa Datenübermittlungen an Drittstaaten aufgrund bestimmter Unternehmensstandards erfolgen sollen.

- Von der Art 29 – Gruppe zum Europäischen Datenschutzausschuss

Die bisher schon bestehende Koordination der datenschutzrechtlichen Kontrollstellen in der sog. Art 29 Gruppe soll durch einen Europäischen Datenschutzausschuss ersetzt werden. Die Funktionen gehen über die bisherigen Stellungnahmemöglichkeiten hinaus. Der Europäische Datenschutzausschuss

---

wenn diese die Aufgabe hat, in dem betreffenden Mitgliedsstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine, mit denen deren Dienstleistung rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen.“ (http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf).

wird noch aktiver in die neuen Verfahren eingebunden und in Datenschutzangelegenheiten noch stärker in Kooperation mit der Europäischen Kommission tätig werden. Durch den Europäischen Datenschutzausschuss wurde der Weg in Richtung einer europäischen Agentur für Datenschutz bereits beschritten. Das europäische Regulierungsmodell kommt daher auch im Datenschutz zunehmend Bedeutung zu.

- EU Kommission

Die Rolle der EU Kommission wird durch die Datenschutz-GrundVO aufgewertet. Zu aller erst sind die Rechtssetzungsbefugnisse im Rahmen der delegierten Akte und der Durchführungsrechtsakte als wichtige Konkretisierungen des geplanten Datenschutzrechts zu nennen.[41] Der den privaten Unternehmen verbleibende Spielraum im Datenschutzrecht wird daher wesentlich durch die EU Kommission bestimmt. Darüber hinaus ist die Europäische Kommission in unterschiedlichen Vollzugsbereichen, insbesondere in Hinblick auf datenschutzrechtliche Standards in Drittstaaten, mit einbezogen.[42] Die Stärkung der Kommission wird etwa auch durch die Stellungnahmekompetenzen im sog. Kohärenzverfahren sichtbar.[43]

- Zusammenfassung

Zusammenfassend zeigt sich, dass die Europäisierung des Datenschutzrechts zu einer Regulierung der wirtschaftsnahen Datenverwendung führt. Auch wenn im Rahmen des Datenschutzrechts keine natürlichen Monopole vorliegen und keine Regulierung von Netzen im engeren Sinn stattfindet,[44] so entsteht ein Typ

[41] Siehe Art. 86 Entwurf.
[42] Siehe Art. 40ff Entwurf.
[43] Siehe Art. 57ff Entwurf.
[44] Siehe *Schneider*, Regulierungsrecht der Netzwirtschaften I (2013) 185ff.

europäischer Verwaltung, der mit dem Regulierungsrecht (etwa im Bereich des Energie- oder Telekommunikationsrechts) vergleichbar ist.[45]

Für die damit verbundenen nationalen Datenschutzbehörden bedeutet dies eine stärkere Entkoppelung von nationalen Strukturen (und damit auch von nationaler demokratischer Legitimation) hin zu einer Agentur-ähnlichen Ausgestaltung, die stärker an europäische Organisationseinheiten gekoppelt ist. In Hinblick auf die Rechtssetzung Privater entsteht durch die Datenschutz-GrundVO ein wesentlich größerer Handlungsspielraum, der sich im Akteur des Datenschutzbeauftragten manifestiert. So begrüßenswert die Einführung eines verpflichtenden betrieblichen Datenschutzbeauftragten anzusehen ist, so hoch ist auch das Risiko, dass damit effektiver Datenschutz erschwert wird.

Die weitere Stärkung der nationalen Datenschutzbehörden, die es ermöglichen effektive Kontrollen durchzuführen, sowie die institutionelle Koppelung staatlichen und betrieblichen Datenschutzes stellen strukturelle Voraussetzungen für die rechtsstaatliche Kontrolle aber auch die Legitimation des Datenschutzrechtes dar. Damit verbunden sind insbesondere auch verfahrensrechtliche Transparenz und die notwendige Ausgestaltung von Rechtsakten erforderlich, um die Kontrolle des rechtlichen Rahmens zu gewährleisten.

[45] Siehe grundlegend zur Schnittstelle des Datenschutz- und des europäischen Wirtschaftsrechts, *Lachmayer,* Datenschutzrecht als Öffentliches Wirtschaftsrecht, in: Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 13 (2013) 9.

3. Verfahren

A. Von Registrierungsverfahren zu Strafverfahren?

Die bevorstehende Abschaffung des Registrierungsverfahrens eröffnet den Gestaltungsspielraum für unternehmerische Entscheidungen. Schon bisher bestand nur ausnahmsweise eine Bewilligungspflicht. Durch die Meldepflicht konnte die Behörde zumindest einen Überblick über die unternehmerischen Tätigkeiten für sich beanspruchen, der nun wegfällt. Es sind daher die verbleibenden bzw entstehenden Verfahren daraufhin zu überprüfen, ob sie in der Lage sind, zumindest teilweise das Meldeverfahren zu ersetzen.

Gem Art 33 Entwurf ist eine sog. Datenschutz-Folgenabschätzung geplant, die das bisherige Bewilligungsverfahren ersetzen soll. Diese Datenschutz-Folgeabschätzung durch Unternehmen wird insbesondere erforderlich, wenn aufgrund des Wesens, Umfangs oder Zweckes einer Datenverarbeitung „konkrete Risiken für die Rechte und Freiheiten betroffener Personen“ bestehen, insbesondere bei Profiling, sensiblen Daten, weiträumiger Videoüberwachung oder Kinderdaten. Dieses Verfahren wäre dazu in der Lage, den Bereich der bisherigen Bewilligung abzudecken bzw. die Bewilligung auf größere Bereiche auszudehnen, womit die rechtliche Absicherung aber damit auch die demokratische Legitimation der Datenverarbeitung durch Unternehmen erhöht werden kann. Wird allerdings diese Bestimmung sehr restriktiv ausgelegt und verbleibt ein großer Spielraum bei den Unternehmen, so wäre damit durch die Vorabgenehmigung nicht viel gewonnen. Die Datenschutz-Folgeabschätzung wird jedenfalls von Unternehmen selbst vorgenommen und der Aufsichtsbehörde zur Genehmigung vorgelegt.

Problematisch an der Datenschutz-Folgeabschätzung bleibt, dass diese durch die Unternehmen selbst zu initiieren ist. Argumentiert ein Unternehmen intern gegen das Bestehen von Risiken kommt es zu keinem Verfahren und keiner Publizität. Es liegt sodann an Betroffenen, sich gegen die Datenanwendungen zu wehren, oder etwa an der besonderen Stellung des Datenschutzbeauftragten, die Datenschutzbehörde zu kontaktieren. Es ist allerdings davon auszugehen, dass es in vielen Fällen zu keinen Verfahren und damit auch zu keiner Vorabgenehmigung kommen wird.

Besteht bei einer Datenanwendung kein Anwendungsfall des Art 33 Entwurf bleibt nur mehr die allgemeine Überwachungsbefugnis der Aufsichtsbehörde gem Art 52 Entwurf bestehen. Die Aufgabe ist generell formuliert und die Befugnisse sind sehr weitreichend. Inwieweit sodann aber auch die Kontrolle ausgeübt wird, hängt vom Ermessen der Behörde einerseits und von der finanziellen und personellen Ausstattung andererseits ab. Es liegt also an der Behörde selbst, die Intensität der Kontrollen zu bestimmen.

Die Kompetenzen der Aufsichtsbehörde beziehen auch Verwaltungsstrafmöglichkeiten mit ein, die gem Art 79 Entwurf äußerst weitreichend ausgestaltet sind und bis zu einer Mio. Euro bzw. 0,5 % des Jahresumsatzes des Unternehmens reichen. Die Änderungen des Europäischen Parlaments würden noch weiterreichende Strafen bis 100 Mio. Euro vorsehen und 5% des Jahresumsatzes betreffen. Der Wegfall der Meldepflicht wird auf diese Weise durch ein sehr weitreichendes Strafrecht kompensiert, das wiederum sehr viel Entscheidungsspielraum bei der Datenschutzbehörde belässt und die Unternehmen zur *compliance* mittels Abschreckung führen soll.

Diese (auch aus demokratischer Sicht) nicht unproblematische Strafgewalt (die ihrerseits weit über andere Strafausmaße hinausreicht) schafft jedenfalls nur

punktuelle Kontrolle, vor allem dann, wenn bereits Beschwerden Betroffener bei der Datenschutzbehörde eingebracht sind. Je nach Handhabung der Strafgewalt kann damit auch ein abschreckendes Instrument entwickelt werden, das zu einer Einhaltung der Regelungen durch Unternehmen führen kann. Wird diese aber etwa aufgrund der Unterfinanzierung der Behörde nicht häufig angewendet, kann – trotz hoher Strafdrohung – die Bedeutung der Strafdrohung sehr gering sein.

B. Auskunftsverfahren

Neben den Verfahren, die durch die Datenschutzbehörde selbst eingeleitet werden, bleibt die richterliche Funktion der Aufsichtsbehörde bestehen. Die betroffene Person hat zu allererst das Recht, bei dem betroffenen Unternehmen Auskunft über die verarbeiteten Daten zu erlangen (§ 26 DSG bzw. Art 15 Entwurf). Gem Art 12 Entwurf legen die Unternehmen selbst das Verfahren zur Auskunft fest. Den Unternehmen wird je nach Entwurf 4-6 Wochen Zeit gegeben, um die Auskunft zu beantworten. Bei Auskunftsverweigerung muss das Unternehmen zumindest über die Beschwerdemöglichkeit an die Aufsichtsbehörde informieren. Empirische Studien zeigen, dass bereits bei der Bereitschaft von Unternehmen, Daten herauszugeben, oftmals Probleme bestehen.[46] Insoweit wären Mindeststandards für das durch die Unternehmen durchgeführte Auskunftsverfahren geboten.

Gem Art 73 Entwurf (bzw. § 31 DSG) kann sich eine betroffene Person an die Aufsichtsbehörde wenden, die bei Auskunftsverweigerung einschreiten kann. Überdies können sich auch NGOs für Betroffene an die Aufsichtsbehörde wenden. Gegen die Entscheidungen der Aufsichtsbehörde bestehen sodann noch

[46] Siehe etwa in Hinblick auf die Videoüberwachung eine Studie von Robert Rothmann http://futurezone.at/netzpolitik/videoueberwachung-nachfragen-nicht-erwuenscht/52.245.601; *Rothmann*, Videoüberwachung und Auskunftsrecht. Eine empirische Analyse visueller Ansprüche, Datenschutz und Datensicherheit 2014, 405.

Möglichkeiten eines gerichtlichen Rechtsschutzes; im konkreten Fall kann sich in Österreich eine betroffene Person gegen den Bescheid der unabhängigen Datenschutzbehörde mittels Beschwerde an das Bundesverwaltungsgericht wenden. Die verfahrensrechtliche Ausgestaltung obliegt sodann den Mitgliedsstaaten; im österreichischen Fall sind somit die Bestimmungen des VwGVG bzw. des AVG anwendbar.

C. Innere und äußere Kontrollen

Mit der Neugestaltung des Datenschutzrechts ist generell eine Verschiebung von äußeren (staatlichen) zu inneren (betrieblichen) Kontrollen verbunden. Als Beispiel dafür dient etwa die Datenschutz-Folgeabschätzung oder die Umsetzung von datenschutzrechtlichen Verhaltensregeln in Unternehmen. Als Zwischenbereich sind externe Kontrollen durch private Institutionen, wie sie etwa in Form von Datenschutzsiegel und Datenschutzzeichen angeboten werden, anzusehen. Da auch die Möglichkeit besteht, den („betrieblichen“) Datenschutzbeauftragten an Dritte (Unternehmen) auszulagern, bestehen unterschiedliche Zwischenformen. Die staatlichen Kontrollen durch die unabhängige Datenschutzbehörde sind, wie geschildert, von diesen privaten Kontrollstrukturen weitgehend abhängig. Nur sehr punktuell in Form von stichprobenartigen Kontrollen oder bei bereits – etwa aufgrund von Verwaltungs(straf)verfahren – bekannten Verletzungen des Datenschutzrechts kann die Datenschutzbehörde eigenständig agieren. Die große Quantität an Problemfällen steht und fällt mit der Kooperation der Unternehmen selbst, die kritisch ihre eigene Datenverwendung auf datenschutzrelevante Sachverhalte überprüfen müssen.

Verfahrensrechtlich bedeutet diese Entwicklung eine Reduktion staatlicher Verfahren, womit auch Transparenz, Einheitlichkeit und Effektivität der Kontrollen

in Frage stehen. Es hängt schließlich viel von den durch die europäische Kommission in Form von Tertiärrechtsakten zu konkretisierenden Vorgaben ab. Werden weitere Konkretisierungen vorgenommen, so kann für außenstehende Personen eine gewisse Transparenz erreicht werden; weitergehende Formen der Partizipation sind allerdings nicht vorgesehen.

D. Europäische Konsultationen

Durch die Einführung spezieller europäischer Konsultationsverfahren, insbesondere in Form des Kohärenzverfahrens, kann es zu einer massiven Ausweitung europäischer Verfahren kommen. Der Europäischen Kommission kommt im Rahmen dieses Verfahrens ein besonderer inhaltlicher Einfluss auf die transnationale Koordinierung zu. Auch in diesem Zusammenhang bedarf es weiterer Konkretisierungen durch Durchführungsrechtsakte der Kommission. Die Relevanz des Kohärenzverfahrens gewinnt insbesondere in Hinblick auf die Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften gem Art 43 Entwurf an Bedeutung, womit es den Unternehmen ermöglicht wird, ihre Daten global innerhalb der Unternehmensgruppe weiter zu verarbeiten.

4. Instrumente

A. Zustimmung und private AGBs

Durch die datenschutzrechtliche Zustimmung Privater begeben sich diese regelmäßig ihrer rechtlichen Möglichkeiten.[47] Dies deshalb, da nur mit der

[47] *Dörfler/Siegwart*, Datenschutz in vertraglichen Beziehungen, in Bauer/Reimer (Hrsg), Datenschutzrecht 509 ff; *Lachmayer*, Die Multidimensionalität des Datenschutzrechts. Zur Notwendigkeit der Ausdifferenzierung datenschutzrechtlicher Regelungen, in: Feik/Winkler (Hrsg), Festschrift für Walter Berka (2013) 121 (133ff).

datenschutzrechtlichen Zustimmung die Verwendung bestimmter Dienste bzw. Vorteile erst möglich wird. Die Zustimmung ersetzt datenschutzrechtliche Prinzipien bzw. Standards. Wer freiwillig seiner Datenverwendung zustimmt, erscheint nicht weiter schützenswert.

Bei näherer Betrachtung ist allerdings zu differenzieren. Ein wesentlicher Grund liegt in der Rechtsetzung durch private Unternehmen in Form von AGBs. Allgemeine Geschäftsbedingungen beinhalten oft datenschutzrechtliche Verfügungen in pauschalierter Form. Den Benutzern bestimmter Dienste steht es auf diese Weise nicht frei zu wählen, welche Daten sie zur Verfügung stellen wollen und welche nicht. Sie sind vielmehr an die datenschutzrechtlichen Vorgaben der AGBs gebunden, um den entsprechenden Dienst nutzen zu können.

Es besteht großer Optimierungsbedarf, um die Nutzer von Diensten in die Lage zu versetzen, selbst über die Verwendung ihrer Daten zu entscheiden.[48] Dafür finden sich unterschiedliche Ansatzpunkte in der Datenschutz-GrundVO. Die Einwilligung zur Verwendung personenbezogener Daten soll gesondert von der Zustimmung zu AGBs ausgewiesen sein und erfolgen.[49] Für Kinder bedarf es eigener Regeln und Grenzen.[50] Insgesamt besteht ein Bedarf für spezifische Regelungen für besonders eingriffsintensive Formen der Datenverarbeitung, etwa in Hinblick auf Profiling[51]. In Hinblick auf den Widerruf der Datenverwendung sind entsprechende Maßnahmen vorzusehen, die verhindern, dass die Datenweitergabe und –verbreitung dazu führt, dass ein Widerruf einer datenschutzrechtlichen Zustimmung *de facto* nicht mehr durchsetzbar ist. Durch die Rsp des EuGH in Hinblick auf ein Recht auf Vergessen wurden neue

[48] Um ein Recht auf informationelle Selbstbestimmung zu gewährleisten, bedarf es der Ausdifferenzierung und nicht der pauschalen Zustimmungen.
[49] Siehe Art. 7 Abs. 2 Entwurf.
[50] Siehe Art. 6 Abs. 5 Entwurf
[51] Siehe Art. 20 Entwurf.

Verpflichtungen geschaffen, um auch ein Widerrufsrecht und damit die Löschung von Daten weiter zu entwickeln.[52]

Von der rechtlichen Ausgestaltung der Zustimmung als rechtliches Instrument sowie von den ergänzenden staatlichen Maßnahmen der Verwendung von Daten Grenzen zu setzen, hängt der Spielraum privater Rechtssetzung ab. Je geringer die Vorgaben für eine ausdifferenzierte Zustimmung ausgestaltet sind, umso schwieriger ist es für den Einzelnen, seine Rechte durchzusetzen bzw. sich gegenüber der Rechtssetzung Privater rechtlich zur Wehr zu setzen und Rechtsschutz zu erlangen.

B. Zertifizierung und Gütesiegel im Datenschutzrecht

Der Ausbau datenschutzspezifischer Zertifizierungsverfahren sowie die Einführung von Datenschutzsiegeln bzw. –zeichen sind ebenfalls im Entwurf zu einer Datenschutz-GrundVO vorgesehen. Die Details der Zertifizierung sollen durch delegierte Rechtsakte der Kommission festgelegt werden. Damit angesprochen sind nicht nur die Bedingungen zu Erteilung und Entzug der Zertifizierung, sondern auch die Anforderungen der Anerkennung von Zertifizierungen innerhalb und außerhalb der Europäischen Union. Die Zertifizierungen basieren sodann wiederum auf technischen Standards, die als private Regelsetzung zu identifizieren sind.[53]

Der Zweck der Zertifizierungsverfahren liegt laut Art 39 Entwurf in der „ordnungsgemäßen Anwendung dieser Verordnung“; die Zertifizierung soll „den

[52] Siehe EuGH 13.5.2014, Rs C-131/12, *Google Spain SL*. Es ist aber auch auf die demokratische Problematik eines Rechts auf Vergessen zu betonen. Ein Recht auf Vergessen kann die Meinungs- und Medienfreiheit signifikant einschränken, indem für öffentliche Personen oder Unternehmen unliebsame Inhalte gelöscht werden.

[53] Siehe etwa ISO 27.001.

Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung“ tragen. Ungeklärt sind allerdings die Rechtswirkung der Zertifizierungen, die Voraussetzung für Zertifizierungen und die Mindeststandards. Es ist davon nicht auszuschließen, dass die Einführung des „New Approach“ im Datenschutzrecht erfolgen wird und aufgrund der Zertifizierung eine datenschutzrechtliche Konformitätsvermutung entstehen könnte.[54] Sollte dieser Weg beschritten werden, so wird die Einhaltung des europäischen Datenschutzrechts weiter relativiert.

C. Verhaltenskodex

Wie schon bisher in Art 27 DatenschutzRL vorgesehen, verstärkt nun Art 38 Entwurf die Förderung von Verhaltensregeln, die durch Branchenvertreter aufgestellt werden. Auf diese Weise wird für Unternehmensvertreter die Möglichkeit geschaffen, eigene Interpretationsmaßstäbe für das Datenschutzrecht zu entwickeln.[55] Diese sind sodann entweder der Aufsichtsbehörde (wenn für einen Mitgliedsstaat) oder der Kommission (für mehrere Mitgliedsstaaten) vorzulegen. Die Kommission kann diesen Verhaltensregeln in weiterer Folge aufgrund von Durchführungsrechtsakten in der Union „allgemeine Gültigkeit“ verleihen. Damit werden die privat konzipierten

---

[54] Siehe zum New Approach und zur Konformitätsvermutung *Holoubek/Fuchs*, Akkreditierung und Zertifierung, in Holoubek/Potacs (Hrsg), Öffentliches Wirtschaftsrecht II (2013) 519 (525ff).

[55] Siehe § 6 Abs 4 DSG sowie Siehe *Dohr/Pollirer/Weiss/Knyrim,* DSG² (2013) § 6 Anm 13; siehe auch die Auseinandersetzung von *Duschanek/Eberhard*, Datenschutzrecht, in Holoubek/Potacs (Hrsg), Öffentliches Wirtschaftsrecht³ (2013) 275 (291). Als Bsp für derartige Verhaltensregeln sind etwa die Verhaltensregeln gem § 6 Abs 4 DSG 2000 für Glückspielbetreiber gem § 14 und § 21 GSPG sowie gem. §22 iVm § 21 GSPG (Konzessionäre) zu nennen, die die „Berufsgruppe Casinos Austria und Lotterien. Fachverband der Banken und Bankiers. Wirtschaftskammer Österreich“ auf ihrer Website publiziert haben (BKA-810.29/0002-V/3/2011) oder die „Verhaltensregeln gem. § 6 Abs 4 DSG 2000 für die Ausübung des Gewerbes gem. § 151 Gewerbeordnung (Adressverlage und Direktmarketingunternehmen)“ des Direkt Marketing Verband Österreich und der WKO Gruppe „Werbung und Marktkommunikation“. Siehe portal.wko.at/wk/dok_detail_file.wk?angid=1&docid...stid; http://www.dmvoe.at/dokumente/CoC-DMV-WK040906.PDF.

Regelungen zu europäischen Standards. Um demokratischen Minimalvorgaben zu genügen, fehlt es dafür aber an der notwendigen Konkretisierung des Verfahrens. Diese könnte durch Einbeziehung unterschiedlicher *stakeholder*, durch Transparenzvorschriften sowie durch spezifische Beschwerdemöglichkeiten erfolgen.

D. Normung im Datenschutzrecht

Das Datenschutzrecht hängt zentral von der technischen Ausgestaltung sowie von Maßnahmen der Datensicherheit ab. Der Entwurf der Datenschutz-GrundVO bekennt sich im 61. Erwägungsgrund zum Grundsatz des Datenschutzes durch Technik und datenschutzrechtliche Voreinstellungen (*data protection by design and default*). Diese Entwicklung ist im Grundsatz zu begrüßen, da auf diese Weise datenschutzrechtliche Vorgaben bereits in der Programmierung Berücksichtigung finden könnten.

Die Verlagerung des Datenschutzes in technische Standards birgt aber auch die Gefahr in sich, dass ohne entsprechenden technischen Sachverstand nicht mehr die Einhaltung datenschutzrechtlicher Regeln erkannt werden kann bzw. technische Sachverständige, etwa Programmierer, über den Datenschutz entscheiden. Auf diese Weise wird der Datenschutz nicht nur schwer kontrollierbar, sondern es wird ihm auch jegliche Form von Legitimation entzogen und Verantwortlichkeiten werden verschleiert. Die Technisierung des Datenschutzes birgt die Gefahr der massiven Reduktion des Datenschutzes in sich, da gesellschaftliche Vorgänge durch technische Prozesse substituiert werden. Es bedarf auch in diesen Fällen weiterhin einer öffentlichen Diskussion über die Schaffung datenschutzrechtlicher Technikstandards und einer externen Kontrolle.[56]

[56] Siehe zur Problematik *Lachmayer*, Technokratische Rechtssetzung Privater, juridikum 2013, 109.

E. Kontrolle durch die Datenschutzbehörde?

Die Erweiterung der Instrumentarien der Rechtssetzung Privater führt potenziell auch zu einer Verringerung der Kontrolle durch die Datenschutzbehörde. Die Einführung zweiter und dritter Ebenen des privaten Datenschutzrechts, die die eigentlichen europäischen datenschutzrechtlichen Vorgaben überlagern, schafft damit auch den Schein der Einhaltung der datenschutzrechtlichen Standards und verlagert Kontrolltätigkeiten auf jene Fälle, bei denen aufgrund der Beschwerden Betroffener ohnedies bereits Verfahren am Laufen sind.

Auch an dieser Stelle bleibt die Notwendigkeit bestehen, die nationale Datenschutzbehörde nicht nur mit entsprechendem juristischen sondern auch mit technischen Sachverstand auszustatten, um die aufgrund komplexer rechtlicher Regelungen und ausgefeilter technischer Systeme bestehende datenschutzrechtliche Ausgangssituation ausreichend analysieren zu können und damit eine effektive Kontrolle zu ermöglichen.

5. Zusammenfassung

Das Datenschutzrecht befindet sich im Umbruch. Die Veränderung und Anpassung des Datenschutzrechts ist aufgrund der beinahe 20 Jahre alten europäischen Regelungen erforderlich. Aus Perspektive der demokratischen Legitimation des Datenschutzrechts bestehen vor allem Herausforderungen der Effektuierung der Einhaltung datenschutzrechtlicher Regelungen. Diese Zielsetzung steht mit der Rechtssetzung durch Private im Datenschutzrecht in einem Spannungsverhältnis. Es sind daher vor allem folgende Problemstellungen relevant:

- Die adäquate personelle und finanzielle Ausstattung der nationalen datenschutzrechtlichen Aufsichtsbehörde ist eine zentrale Voraussetzung für die Durchführung datenschutzrechtlicher Kontrollen. Diese werden bei Wegfall der Meldepflicht umso wichtiger.

- Die Einführung von betrieblichen Datenschutzbeauftragten soll nicht dazu führen, dass unterhalb der dafür vorgesehenen Schwelle (etwa von 250 Mitarbeitern im Unternehmen) dem Datenschutzrecht keine Bedeutung mehr zukommt. Überdies sind die Unabhängigkeitsgarantien der Datenschutzbeauftragten ebenso wie die Zusammenarbeit mit der nationalen datenschutzrechtlichen Aufsichtsbehörde zu stärken.

- Zentrale Bedeutung zur Effektuierung des Datenschutzes kommt der Information der Betroffenen und der Möglichkeit zur Auskunft zu. Insoweit sind entsprechende Auskunftsverfahren auch von europäischer bzw. staatlicher Seite vorzugeben und sind nicht der jeweiligen betrieblichen Konzeption zu überlassen. Die Öffentlichkeit und Transparenz im Umgang mit Datenverarbeitungen sollte diesbezüglich gestärkt werden.

- Das zentrale rechtliche Instrument der Verwendung personenbezogener Daten ist die datenschutzrechtliche Zustimmung. Hier bedarf es einer weitergehenden Konkretisierung der Zustimmung, etwa in Form der Ausdifferenzierung von Zustimmung zu einzelnen Datenverwendungen oder der stärkeren Ausgestaltung der Zustimmung bei Kindern.

- Auch das Widerrufsrecht und die Einführung eines Rechts auf Vergessen durch ein verstärktes Löschungsrecht stellen zentrale Mittel zur Stärkung der Verbrauchermöglichkeiten dar.

- Die Einführung von Verhaltenskodices, Zertifizierungsverfahren, Gütesiegeln und technischen Standards im Datenschutzrecht birgt einerseits die Gefahr der Verschleierung der Einhaltung der rechtlichen Datenschutzstandards in sich, andererseits kann sie zur Reduktion der datenschutzrechtlichen Kontrollen führen. In beiden Fällen würde das Datenschutzrecht an Effektivität verlieren.

- Die Kompensation der reduzierten staatlichen Kontrolle im Datenschutzrecht durch ein weitreichendes Verwaltungsstrafrecht scheint nur punktuell in der Lage zu sein, die Einhaltung der datenschutzrechtlichen Standards zu gewährleisten. Überdies ist ein derartiges Verwaltungsstrafrecht einer bereits von der staatlichen Verwaltung ausgegliederten und unabhängigen Datenschutzbehörde für sich genommen aus demokratischer Perspektive problematisch.

Bibliografie

Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, ÖJT GA I/1 (2012)

von Bogdandy, Grundprinzipien, in ders/Bast (Hrsg), Europäisches Verfassungsrecht² (2009) 13

Bresich/Riedl/Souhrada-Kirchmayer, Die völlig unabhängige Datenschutzkontrollstelle, ZfRV 2014, 52

Dohr/Pollirer/Weiss/Knyrim, DSG² (2013).

Dörfler/Siegwart, Datenschutz in vertraglichen Beziehungen, in Bauer/Reimer (Hrsg), Datenschutzrecht (2009) 509

Duschanek/Eberhard, Datenschutzrecht, in Holoubek/Potacs (Hrsg), Öffentliches Wirtschaftsrecht³ (2013) 275

Hötzendorfer/Schweighofer, Safe Harbour in der „Post-Snowden-Ära", in Lück-Schneider ua (Hrsg), Gemeinsam Electronic Government ziel(gruppen)gerecht gestalten und organisieren (2014) 125

Grabenwarter, Die demokratische Legitimation weisungsfreier Kollegialbehörden in der staatlichen Verwaltung. Zur Zulässigkeit der Entsendung von Organwaltern durch nicht demokratisch legitimierte Einrichtungen, in Haller ua (Hrsg) Staat und Recht. FS Winkler (1997) 271

Grabenwarter/Holoubek, Demokratie, Rechtsstaat und Kollegialbehörden mit richterlichem Einschlag. Zu den verfassungsrechtlichen Grenzen der Einrichtung von Kollegialbehörden nach Art 20 Abs 2 und Art 133 Z 4 B-VG, ZfV 2000, 194

Holoubek/Fuchs, Akkreditierung und Zertifierung, in Holoubek/Potacs (Hrsg), Öffentliches Wirtschaftsrecht II (2013) 519

Jahnel, Handbuch Datenschutzrecht (2010)

Kimm, Rechtsschutz im Datenschutz, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 153

Kotschy, Die Änderungen im Registrierungsverfahren nach der DSG-Novelle 2010, in N. Raschauer (Hrsg), Datenschutzrecht 2010 (2011) 51

Kuner, European Data Protection Law: Corporate Compliance and Regulation (2007)

Lachmayer, Zur Reform des Europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, Österreichische Juristenzeitung 2012, 841

Lachmayer, Technokratische Rechtssetzung Privater, juridikum 2013, 109

Lachmayer, Die Multidimensionalität des Datenschutzrechts. Zur Notwendigkeit der Ausdifferenzierung datenschutzrechtlicher Regelungen, in: Feik/Winkler (Hrsg), Festschrift für Walter Berka (2013) 121

Lachmayer, Datenschutzrecht als Öffentliches Wirtschaftsrecht, in: Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 13 (2013) 9

Lee Bygrave, Data Privacy Law. An International Perspective (2014)

Müller, „Agentur hat Konjunktur" – „Agencification" und demokratische Verwaltungslegitimation", JBÖffR 2011, 261

Navacchi, Die Registrierung von Datenanwendungen, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 195

Öhlinger/Eberhard, Verfassungsrecht[10] (2014)

Radin, *Boilerplate* (2013)

Raschauer, Art 20 Abs 1 B-VG, in Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht. Kommentar 3. Lfg (2000).

Rothmann, Videoüberwachung und Auskunftsrecht. Eine empirische Analyse visueller Ansprüche, Datenschutz und Datensicherheit 2014, 405

Rill, Art 18 B-VG, in Kneihs/Lienbacher (Hrsg), Rill-Schäffer-Kommentar. Bundesverfassungsrecht 1. Lfg. (2001)

Schneider, Regulierungsrecht der Netzwirtschaften I (2013)

Souhrada-Kirchmayer, Der Entwurf eines neuen Datenschutz-Rechtsrahmens der Europäischen Union, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government 2012 (2012) 9

Westphal, Grundlagen und Bausteine des europäischen Datenschutzrechts, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 53