Schriften zum Öffentlichen Recht

Band 1426

Der Grundsatz digitaler Souveränität

Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung

Von

Christian Ernst

Duncker & Humblot · Berlin

CHRISTIAN ERNST

Der Grundsatz digitaler Souveränität

Schriften zum Öffentlichen Recht

Band 1426

Der Grundsatz digitaler Souveränität

Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung

Von

Christian Ernst

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Satz: 3w+p GmbH, Rimpar
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-15931-4 (Print)
ISBN 978-3-428-55931-2 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Geleitwort

Können Sie sich noch an die in den achtziger Jahren geplante Volkszählung erinnern? Mit Befragern an der Haustür sollten vor allem Haushaltsgrößen ermittelt werden. Massive Proteste behinderten damals die Durchführung. Man fürchtete, zum „gläsernen Menschen“ zu werden. Heute liefert schon das Einschalten Ihres Smartphones ein Vielfaches der Daten aus, die damals so vehement verweigert wurden. Es scheint, als habe die Digitalisierung in kürzester Zeit zu einer vollkommen anderen Wahrnehmung von Sicherheitserfordernissen und Persönlichkeitsschutzrechten geführt. Die Menschen gehen mit ihren Daten und mit Daten über sie vor allem dann einigermaßen bedenkenlos um, wenn sie es mit Geräten, Apps und Leistungen privater Anbieter zu tun haben. Google, Facebook, Amazon und Apple werden permanent ungeheure Datenmengen geschenkt. Daten, die Spiegel unserer Selbst sind, die uns mitunter besser und treffender beschreiben als dies gute Freunde tun könnten. Die uns vor allem auch wortwörtlich berechenbar machen.

Man mag diesen geradezu freiwilligen Verlust digitaler Souveränität im privaten Bereich bedauern. Mit Blick auf Daten, die vom Staat verarbeitet werden, ist er inakzeptabel. Man stelle sich vor, Meldedaten oder Daten der Finanzverwaltung würden über US-amerikanische Server von Unternehmen laufen, die daraus Erkenntnisse zur Maximierung ihres Geschäftserfolgs gewinnen würden. Was hier spontan abwegig erscheint, ist jedoch mithin möglich. Denn die technisch notwendigen Fähigkeiten zur Entwicklung und Beherrschung einer IT mit den hohen Anforderungen an Sicherheit und Verfügbarkeit, wie sie an staatliche Datenverarbeitung geknüpft sind, übersteigen die Möglichkeiten einzelner staatlichen Stellen. Es wäre auch, wie es im nachfolgenden Gutachten heißt, „in höchstem Maße ineffizient, würde jede einzelne zuständige Stelle selbst vollumfänglich ausreichende technische Fähigkeiten für die notwendige Datenverarbeitung vorhalten“ (15).

Als Alternative bietet sich somit die Beschaffung externer Kapazitäten an (15). Es liegt jedoch in ihrer technischen Natur, dass Daten „schlüpfrig“ sind: Sie sind schnell, ohne nennenswerten Aufwand und mit geringen Kosten zu übertragen – und mit jeder Übertragung und jeder Zugriffsmöglichkeit wächst die Gefahr, dass Daten den Weg in die Öffentlichkeit finden. Und während Kontrolle bei anderen Aufgabenprivatisierungen zumindest im Nachhinein wiederherstellbar ist, können die Folgen von Datenverlust oder -missbrauch häufig nicht mehr rückgängig gemacht werden (40). Die nachträgliche Missbrauchskontrolle, die sonst üblich ist, greift bei Daten nicht (76).

Und werden staatliche Daten an einen privaten IT-Dienstleister übermittelt, sind zumindest außerbehördliche Zugriffsmöglichkeiten möglich. Keine Frage, dass dies

besondere Vorkehrungen erforderlich macht. Die Verantwortlichkeiten müssen dabei klar geregelt sein und verbindlich vereinbart werden. Das vorliegende Gutachten beschreibt ausführlich, welche Kriterien und Maßstäbe dabei anzulegen sind, welche Risiken mithin dabei „eingekauft" werden.

Der Wunsch nach Erhalt der digitalen Souveränität durch staatliche Akteure besteht im wahrsten Sinne des Wortes zu Recht: Denn digitale Souveränität ist ein Rechtsprinzip – verfassungsrechtlich und einfachgesetzlich gegründet. Der Staat hat, anders als die gewinnorientierten Datensammler der Internetökonomie, kein geschäftliches Interesse an den Daten der Bürgerinnen und Bürger. Die Behörden arbeiten mit diesen Daten, um zum Beispiel Aufgaben der Steuerverwaltung, des Meldewesens oder der Arbeits- und Sozialverwaltung zu erledigen. Damit die Informationsmacht des Staates begrenzt ist, bestimmt allein die Aufgabenerfüllung den Zweck der Datenverarbeitung: Staatsfinanzierung, Sicherheit, Ordnung, Fürsorge. Die Grundwerte unserer Verfassung, Menschenwürde, Gleichberechtigung, soziale Teilhabe, demokratische Mitgestaltung, Rechtsstaatlichkeit und Beteiligung der Sozialpartner müssen die Richtschnur bei der Entwicklung digitaler Geschäftsprozesse der staatlichen Verwaltung sein.

Denn es ist die Aufgabe des Staates, die digitale Souveränität der Bürgerinnen und Bürger zu schützen und zu gewährleisten. Und seine eigene digitale Souveränität – denn auch diese ist gefährdet, wenn Algorithmen, Analysetechnologie und Infrastruktur überwiegend oder gar allein in den Händen großer Technologiekonzerne liegen, die mitunter weder europäischen Rechtsnormen unterliegen noch unseren ethischen Maßstäben verpflichtet sind.

So stellt sich den Trägern öffentlicher Gewalt also die Frage, welcher Weg der Staat zur Aufrechterhaltung und Entwicklung einer leistungs- und zukunftsfähigen Informationstechnik beschreiten sollte und beschreiten kann. Denn neben rein privaten IT-Dienstleistern gibt es auf der Ebene des Bundes, der Länder und Kommunen viele IT-Dienstleister, die von der öffentlichen Hand getragen werden. In einzelnen Sachbereichen herrscht hierzu eine einfachgesetzliche Rechtslage, etwa die §§ 17 Abs. 3,2 Abs. 2 FVG für die Finanzverwaltung oder für die digitale Führung des Grundbuchs entsprechend § 126 Abs. 3 GBO (15). Abseits solcher Einzelfallregelungen fehlt es jedoch an generellen Vorgaben. Dabei bedarf das Ringen nach digitaler Souveränität gerade jetzt, auf dem unumkehrbaren Weg in die Digitalisierung der Verwaltung, solch allgemeingültiger Direktiven. Staatliche Souveränität – und damit auch die digitale Souveränität des Staates – hat Verfassungsrang. Jedoch stellen die materiellen Verfassungsnormen im Hinblick auf die Teilung von Aufgaben zwischen staatlichen und privaten Dienstleistern nicht mehr als eine Rahmenordnung bereit. Somit bleiben unterschiedlichste Konstellationen und Formen der Verarbeitung von Daten der Bürgerinnen und Bürger möglich. Bis hin zu solchen, die daran zweifeln lassen, ob der Staat noch ein von ihm gesteuertes und damit auch rechtlich gebundenes digitales Verwaltungshandeln gewährleisten kann. Nicht umsonst wird der Ruf lauter nach einer Harmonisierung der verwaltungsrechtlichen

Digitalnormen, die über eine Vielzahl von Einzelgesetzen (VwVfG, eGovG, OZG, DSGVO, Fachgesetze etc.) verstreut sind.

Als Anstoß zu einer dringend erforderlichen Diskussion dahingehend haben wir das nachfolgend veröffentlichte Gutachten in Auftrag gegeben. Die zentrale Fragestellung der wissenschaftlichen Ausarbeitung ist: „Wie kann die digitale Souveränität des Staates selbst im Kontext der zunehmenden Digitalisierung sichergestellt werden?"

Das Gutachten zeigt eindrucksvoll das Spannungsfeld, in dem sich die staatliche Informationsverarbeitung bewegt: Einerseits ist der Schutzauftrag des Staates in Deutschland hinsichtlich der digitalen Souveränität seiner Bürgerinnen und Bürger verfassungsrechtlich gegründet in den objektiv-rechtlichen Schutzgehalten diverser Grundrechte sowie des Staatsauftrags. Auf der anderen Seite braucht es jedoch ein begründetes Vertrauen der Bürgerinnen und Bürger in die digitale Selbstbestimmung und Handlungsfreiheit des Staates selbst – sowie darin, dass persönliche Daten ausschließlich im Rahmen der Zweckbindung genutzt werden. Eine entsprechende Gewährleistungsverantwortung des Staates muss die Gemeinwohlverträglichkeit einer Aufgabenerfüllung durch private Akteure sicherstellen – was gerade bei der Datenverarbeitung mit besonderen Schwierigkeiten verbunden ist.

Ohne Vertrauen gibt es keine Akzeptanz der Online-Verwaltung. Mehr noch: Der Autor formuliert, dass „ein allgemeines Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen als zwingende Voraussetzung für den demokratischen Rechtsstaat angesehen werden" kann (68). Dass aber auch ein besonderes Maß an Vertrauen gerade in solchen Bereichen notwendig ist, „die sich neu entwickeln, für den Einzelnen unbekannt sind und für die Erfahrungen fehlen" (67) – also gerade im Zuge des aktuell stattfindenden Umbruchs von herkömmlichen zu digitalen Prozessen, der Digitalisierung.

Und gerade dieses Vertrauen geht schnell verloren. Während man auch schon beinahe verniedlichend von „Datenpanne" spricht, wenn Facebook millionenfach persönliche Daten „verliert", würden Fehler in weitaus geringerem Maße im Zusammenhang mit staatlicher IT den Glauben an die Gemeinwohlverpflichtung der Verwaltung insgesamt erschüttern.

Der Autor des Gutachtens stellt fest: „Es fehlen generelle und allgemeingültige Vorgaben, in welchen Konstellationen Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen dürfen" (16). Sie sehen insbesondere unter dem Aspekt eines drohenden Vertrauensverlustes in die Integrität und Leistungsfähigkeit staatlicher IT, dass ein vertrauensvoller Umgang mit Daten nur dann möglich ist, „wenn von vornherein und eindeutig klar ist, dass diese in einem öffentlich-rechtlich geprägten Herrschaftsbereich verbleiben, der durch unmittelbare Grundrechts- und Gesetzesbindung gekennzeichnet ist" (76).

Ich freue mich sehr, Ihnen mit dem nachstehenden Gutachten eine wissenschaftliche Sicht auf den Sachkomplex zu präsentieren, die in einer beherzt geführten

Diskussion für mehr Klarheit sorgt. Sie verschafft Ihnen damit mehr Entscheidungssicherheit bei einer Aufgabe, die eine der wohl weitreichendsten staatlichen Aufgaben des 21. Jahrhunderts ist – die Wahrung unserer digitalen Souveränität.

Hamburg/Altenholz, im Oktober 2019 *Dr. Johann Bizer*
Vorstandsvorsitzender Dataport

Vorwort

Das vorliegende Gutachten habe ich im Auftrag von Dataport AöR erstellt. Ausgangspunkt war der Eindruck, dass die Frage, wann und in welchem Ausmaß sich Träger öffentlicher Gewalt bei der Wahrnehmung ihrer Aufgaben privater IT-Dienstleister bedienen dürfen, in der Rechtswissenschaft kaum geklärt ist, insbesondere im Hinblick auf grundsätzliche Strukturen, die diesem Bereich zugrunde liegen. Dabei liegt es auf der Hand, dass dieser Frage im Zuge der fortschreitenden Digitalisierung der öffentlichen Verwaltung eine erhebliche Relevanz zukommt. Denn mit der zunehmenden Bedeutung von Informationstechnologien können auch die Unternehmen, die über diese Technologien verfügen und sie der öffentlichen Hand zur Verfügung stellen, einen stetig wachsenden Einfluss auf die Ausübung staatlicher Befugnisse erhalten.

Dass es sich hierbei nicht nur um theoretische Überlegungen handelt, zeigt sich immer deutlicher. So war unlängst zu erfahren, dass die Bundespolizei die Aufnahmen ihrer Bodycams in einer Amazon-Cloud speichert. Das Unternehmen ist nicht nur der prägende Akteur im Online-Einzelhandel, sondern als Amazon Web Services auch führender internationaler Anbieter von Cloud Computing. Und im Rahmen des Ausbaus des 5G-Netzes diskutieren Fachkreise öffentlich, ob die Mitwirkung des chinesischen Netzwerkausrüsters Huawei ein Sicherheitsproblem darstellt. Angesichts dieser Entwicklung liegt die Frage, ob private Unternehmen einen unverhältnismäßig großen und möglicherweise gefahrbringenden Einfluss auf die Funktionsfähigkeit der Verwaltung oder grundlegender Infrastrukturen bekommen, nahe.

Herrn Johannes Franke danke ich für wertvolle Unterstützung und Diskussionen. Frau Pauline Rachor danke ich für Hilfe bei der Erstellung des Manuskripts.

Hamburg, Oktober 2019 *Christian Ernst*

Inhaltsverzeichnis

A. Einleitung

Für Träger staatlicher Gewalt ist die Verwendung von Daten untrennbar mit der alltäglichen Aufgabenwahrnehmung verbunden. Dabei übersteigen die technisch notwendigen Fähigkeiten immer öfter die Möglichkeiten einzelner staatlicher Stellen, die für die spezifische Aufgabenwahrnehmung zuständig sind. Für die Staatsgewalt wäre es – ebenso wie für viele Private – in höchstem Maße ineffizient, würde jede einzelne zuständige Stelle selbst vollumfänglich ausreichende technische Fähigkeiten für die notwendige Datenverarbeitung vorhalten.

Als Alternative bietet sich die Beschaffung externer Kapazitäten an. Werden staatliche Daten an einen privaten IT-Dienstleister übermittelt, können sich dadurch aber tatsächliche Zugriffsmöglichkeiten des Privaten auf die staatlichen Daten ergeben. Dies kann besondere Vorkehrungen erforderlich machen. Zugleich existiert mittlerweile auf den Ebenen des Bundes, der Länder und der Kommunen sowie anknüpfend an einzelne Sach- und Geschäftsbereiche eine Vielzahl öffentlicher IT-Dienstleister. Im Hinblick auf solche Formen des IT-Outsourcing[1] stellt sich Trägern öffentlicher Gewalt deshalb stets die Frage, ob sie IT-Dienstleister, die von der öffentlichen Hand getragen werden, oder private IT-Dienstleister in Anspruch nehmen.

Die Praxis zeichnet ein differenziertes Bild. Teilweise scheint die öffentliche Gewalt keine gesteigerten Berührungsängste vor privaten IT-Dienstleistern zu haben. Ein Beispiel bildet die Zusammenarbeit der Bundespolizei mit Amazon Web Services bei der Speicherung der Aufnahmen von Bodycams.[2] In anderen Fällen hingegen werden Vorbehalte gegen die Einbindung privater IT-Unternehmen auch in der Öffentlichkeit breit diskutiert, etwa solche gegen die Einbeziehung des chinesischen Netzwerkausrüsters Huawei beim Aufbau des 5G-Netzes.

Die Rechtsordnung gibt auf die Frage, ob ein Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen darf, lediglich für einzelne Sachbereiche eine ausdrückliche Antwort.[3] Für die Finanzverwaltung etwa bestimmen die §§ 17 Abs. 3, 2 Abs. 2 FVG, dass nur Rechenzentren der Landesfinanzverwaltung mit Datenverarbeitungsaufgaben betraut werden dürfen und für die digitale Führung des Grundbuchs erlaubt § 126 Abs. 3 GBO unter bestimmten Umständen eine externe Datenverarbeitung (lediglich) auf den Anlagen einer anderen staatlichen Stelle oder

[1] Zum Begriff des IT-Outsourcing *Heckmann*, in: Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, Teil 10 Rn. 1 ff.; *Ulmer*, CR 2003, 701 (702). Vgl. auch *Zundel*, CR 1996, 763.

[2] BT-Drs. 19/8180, S. 15, 22.

[3] Vgl. auch Nr. 2 des Beschluss Nr. 2015/5 des Rates der IT-Beauftragten der Ressorts vom 29. 7. 2015.

auf den Anlagen einer juristischen Person des öffentlichen Rechts. § 30 Abs. 9 AO lässt mittlerweile eine Auftragsverarbeitung i.S.d. DSGVO nur dann zu, wenn die Daten ausschließlich durch Personen verarbeitet werden, die zur Wahrung des Steuergeheimnisses verpflichtet sind. Nach § 30 Abs. 1 AO sind damit grundsätzlich Amtsträger angesprochen und § 30 Abs. 3 AO erweitert dies auf die für den öffentlichen Dienst besonders verpflichteten Personen (vgl. § 11 Abs. 1 Nr. 4 StGB).

Abseits solcher Einzelfallregelungen werden die Voraussetzungen und Schranken einer Inanspruchnahme privater IT-Dienstleister durch Träger staatlicher Gewalt bislang kaum diskutiert und problematisiert.[4] Es fehlen generelle und allgemeingültige Vorgaben, in welchen Konstellationen Träger staatlicher Gewalt private IT-Dienstleister in Anspruch nehmen dürfen. Den dahinterstehenden Fragen soll die vorliegende Untersuchung nachgehen.

Bei diesem Vorgehen wird ein Grundsatz digitaler Souveränität deutlich werden, der zur Konsequenz haben kann, dass Daten ausschließlich in einer öffentlich-rechtlich geprägten Herrschaftssphäre verbleiben müssen und nicht Privaten übertragen werden dürfen. Bestehende einfachgesetzliche Regelungen, die in diese Richtung zielen, lassen sich als Konkretisierung dieses Grundsatzes verstehen.

[4] Ebenso *Heckmann*, in: ders. (Hrsg.), jurisPK-Internetrecht, Kap. 5 Rn. 164; *ders./Braun*, BayVBl. 2009, 581 (581); vgl. *Petri/Dorfner*, ZD 2011, 122 (127). Vgl. zu den konkreten Modalitäten einer Privatisierung *Schubert*, Privatisierung des eGovernments, S. 201 ff.