30. November 2018

Datensouveränität als Bestandteil des Once-Only-2.0-Prinzips

Datensouveränität als digitale Daseinsvorsorge

Durch die voranschreitende Digitalisierung und wachsende Abhängigkeit der Menschen von digitalen Produkten und Infrastrukturen kommt dem Datenschutz eine immer wichtigere Rolle bei der Sicherung von Rahmenbedingungen für selbstbestimmtes Handeln zu. Der Datenschutz „schützt" dabei nicht die Daten, sondern dient der Ermöglichung der informationellen Selbstbestimmung. So gibt die europäische Datenschutz-Grundverordnung (DSGVO) richtungsweisend den rechtlichen Rahmen für die Verarbeitung von personenbezogenen Daten vor.

Der Begriff „Datensouveränität" geht dabei allerdings weiter als normative Rahmenbedingungen für die Ausübung des Rechts auf informationelle Selbstbestimmung und zielt darauf aufbauend auf die Befähigung des Nutzers ab, selbstbestimmt, informiert und umfassend über die Verwendung seiner Daten zu entscheiden und gleichzeitig an dem „Ertrag" der Verwendung seiner Daten möglichst gleichberechtigt zu partizipieren.[1] Datensouveränität zu ermöglichen heißt daher, für BürgerInnen Vertrauensanker für einen souveränen Umgang mit ihren Daten zu schaffen. Sie wird gewährleistet, indem man die Einhaltung von Datenschutzregeln sicherstellt, technologische Instrumente für ein selbstbestimmtes Handeln im Netz bereitstellt und digitale Kompetenzen vermittelt. So könnte die Gewährleistung der Datensouveränität – analog zur Sicherheit oder Bildung – auch als Teil der Daseinsvorsorge und damit auch als öffentliches Gut aufgefasst werden, das eine besondere Verantwortung und Schutzpflicht des Staates impliziert.

Transparenz und Kontrolle – die wichtigsten Bausteine der Datensouveränität

Zu den wesentlichen Aspekten der informationellen Selbstbestimmung gehört, dass das Individuum jederzeit wissen können muss, wer, zu welchen Zwecken und für wie lange seine Daten verarbeitet, und der Datenverarbeitung unter Umständen entweder zustimmen oder widersprechen kann. Transparenz und

[1] Vgl. Horn, Nikolai & Reinhardt Marc (2018): Datenhoheit – Gerechtigkeitsfrage in einer Digitalen Gesellschaft, URL: https://initiatived21.de/app/uploads/2018/10/denkimpuls_datenhoheit.pdf (letzter Abruf: 30.11.2018).

Autoren: Marc Reinhardt, Initiative D21 e. V. / Capgemini, Dr. Nikolai Horn, Capgemini

Kontrolle sind damit zwei wesentliche Aspekte der informationellen Selbstbestimmung und der Datensouveränität. Die Transparenz kann dabei als notwendige Voraussetzung für die Datenkontrolle betrachtet werden: Nur wenn die BürgerInnen wissen, welche personenbezogenen Daten, von wem und zu welchen Zwecken verarbeitet werden, können sie ihre digitalen Kontroll- und Interventionsrechte aktiv wahrnehmen. Damit wird die Hoheit der BürgerInnen über ihre personenbezogenen Daten gewährleitet.

Datensouveränität bei digitalen Verwaltungsangeboten und Once-Only-Prinzip

Aufgrund der besonderen staatlichen Verantwortung bei der Gewährleistung der Datensouveränität tragen die öffentlichen Stellen eine besonders hohe Verantwortung für den Umgang mit personenbezogenen Daten der BürgerInnen. Mit der Gewährleistung der Datensouveränität hängt die Akzeptanz von digitalen Plattformen zusammen: Hohe Transparenz und Datenkontrolle führt zur Nachvollziehbarkeit von Verwaltungsprozessen und schafft Vertrauen der BürgerInnen in staatliche Angebote.

Das gilt auch für die Umsetzung des Once-Only-Prinzips. Mit dem Once-Only-Prinzip soll erreicht werden, dass BürgerInnen und Unternehmen bestimmte Standardinformationen den Verwaltungsbehörden nur einmal mitteilen müssen, da diese die Informationen untereinander austauschen (Once-Only 1.0). Die Idee des Once-Only 2.0 geht dabei noch weiter und zielt auf die Einbeziehung der bereits vorliegenden Daten aus der Wirtschaft in die Verwaltungsprozesse. Denn eine stärkere Nutzung von Daten ermöglicht Mehrwerte. Die Verwaltung kann damit künftig zur zentralen Drehscheibe beim Datenfluss zwischen staatlichen Stellen, Unternehmen und BürgerInnen werden.

Once-Only 2.0 kann nur dann funktionieren, wenn Datenflüsse ermöglicht werden. Die Datenflüsse dürfen jedoch nur dann ermöglicht werden, wenn sie im Hinblick auf die Datensouveränität der BürgerInnen verantwortungsvoll ausgestaltet sind. Gerade wenn es um den Zugang von Behörden zu privaten Daten (wie bspw. Mietverträge, Rechnungen, Versicherungsunterlagen oder medizinische Unterlagen) geht, herrschen bei den BürgerInnen Bedenken vor, die vor allem in den Sorgen um die „gläserne BürgerInnen“ begründet sind.[2] Aus diesem Grund muss die Gewährleistung der Datensouveränität als integraler Bestandteil bei der Umsetzung des Once-Only-2.0-Prinzips begriffen werden. Wenn der Staat bei der lebenslagenbezogenen Digitalisierung seiner Leistungen konsequente Datenweitergabe zwischen Öffentlichen und Privaten ermöglichen soll, muss er gleichzeitig eine neue Qualität bei Transparenz und Nutzungskontrolle ermöglichen.

[2] eGovernment MONITOR 2018, Nutzung und Akzeptanz von Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, S. 40, URL: https://initiatived21.de/publikationen/egovernment-monitor-2018/ (letzter Zugriff: 30.11.2018).

Mit der Ermöglichung der Transparenz über die Datennutzung und den Kontroll- und Steuerungsmöglichkeiten der Datenverwendung bei digitalen Verwaltungsangeboten kann der Staat mit gutem Beispiel vorangehen. Der Mehrwert für die BürgerInnen ergibt sich zum einen aus den lebenslagenbezogenen Verwaltungsangeboten, die mehr Komfort und Zeitersparnis ermöglichen. Zum anderen aus der Gewissheit, dass mit dem Staat als Garant für die Gewährleistung der Datensouveränität die Daten nicht in Sphären geraten, wo sie faktisch unkontrollierbar verarbeitet, ausgewertet und für unüberschaubare Zwecke eingesetzt werden. Mit dem gewonnenen Vertrauen der BürgerInnen kann der Staat dann auch in einer Vorbildrolle gegenüber der Wirtschaft auftreten.

Technologische Ansätze für mehr Transparenz und Datenkontrolle

Doch wie kann in der praktischen Umsetzung des Once-Only-2.0-Prinzips sichergestellt werden, dass die BürgerInnen durch verbesserte Transparenz- und Kontrollmöglichkeiten zu souveränen Akteuren werden? Dafür empfiehlt es sich, technologische Instrumentarien und Tools zu nutzen, um Datenschutz und Datenbewusstsein nutzungsfreundlich und intuitiv (nutzerzentriert) zu gestalten. Es gibt bereits einige Ansätze, welche die Stärkung der Datensouveränität durch datenschutzfreundliche Technologien voranzutreiben suchen. Diese sind vor allem unter dem Begriff „Privacy Information Management Systems“ (PIMS) bekannt. Mit PIMS-Ansätzen wird versucht, bessere Transparenz- und Kontrollmechanismen technisch zu entwickeln und so die informationelle Selbstbestimmung der NutzerInnen zu stärken. Auch der EU-Datenschutzbeauftragte empfiehlt in seiner Stellungnahme zur Umsetzung des Once-Only-Prinzips den Einsatz von technischen PIMS-Ansätzen zur Steigerung der Transparenz und zur Ermöglichung besserer Nutzerkontrolle beim Ausbau zentraler Zugriffsstellen in der öffentlichen Verwaltung.[3]

Auf der technischen Seite sollen die BürgerInnen ex ante mit Hilfe eines Einwilligungsassistenten gemäß ihren individuellen Privacy-Präferenzen Einstellungen zu Kategorien der Datenempfänger und Verarbeitungszwecken vornehmen können und in die Datenverarbeitung *informiert* einwilligen.[4] Ex post sollen die BürgerInnen im einer Art „Privacy-Cockpit“ einsehen können, welche Institutionen in der Vergangenheit auf ihre Daten zugegriffen haben (Logging der Zugriffe und Austausche), ihre Privacy-

[3] Stellungnahme (08/2017) des EDSB zu dem Vorschlag für eine Verordnung über die Einrichtung eines zentralen digitalen Zugangstors und den Grundsatz der „einmaligen Erfassung“, S. 12 f. URL: https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_de.pdf (letzter Zugriff: 30.11.2018).
[4] Zur Ermöglichung der informierten Einwilligung durch s.g. „Einwilligungsassistenten“ siehe Studie der Stiftung Datenschutz: Horn/Riechert/Müller: „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“. URL: https://stiftungdatenschutz.org/themen/pims-studie/ (letzter Zugriff: 30.11.2018).

Einstellungen dynamisch anpassen und ihre Betroffenenrechte (Löschung, Auskunft etc.) ausüben können. Auch der diesjährige eGovernment MONITOR zeigt, dass Transparenz für die Onliner die wichtigste Funktion bei der idealen Ausgestaltung eines Bürgerkontos ist: Sechs von zehn wünschen sich, jederzeit sehen zu können, welche Behörde wann auf welche Dokumente zugegriffen hat. Knapp die Hälfte möchte unterschiedliche Zugriffsrechte je nach Behörde vergeben.[5]

Der Einsatz von Privacy-Assistenten würde die Erfüllung der Grundprinzipien der Transparenz und der Datenkontrolle in einer Once-Only-2.0-Plattform ermöglichen und damit die Akzeptanz und das Vertrauen der BürgerInnen stärken. Beim Ausbau des Once-Only-2.0-Prinzips müssen jedenfalls der/die einzelne BürgerIn als Mittelpunkt, der Staat als Garant seiner Datensouveränität und Unternehmen als Partner verstanden werden.

[5] eGovernment MONITOR 2018, Nutzung und Akzeptanz von Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, S. 38ff., URL: https://initiatived21.de/publikationen/egovernment-monitor-2018/ (letzter Zugriff: 30.11.2018).