Recht

Private einbinden?

[24.02.2020] Der Grundsatz digitaler Souveränität kann dazu führen, dass staatliche Daten nicht an private IT-Dienstleister übertragen werden dürfen. Der Beitrag informiert über die Risiken beim Einbinden Privater in die Aufgabenwahrnehmung der öffentlichen Hand.

Informationstechnologien bestimmen mittlerweile nicht nur den Alltag der Bürger, auch die öffentliche Verwaltung kann ohne ihren Einsatz nicht mehr gedacht werden. Doch aufgrund von Personalnot oder dem Druck, die alltäglichen Aufgaben zu erfüllen, muss die Aneignung technischer Kenntnisse und Fähigkeiten gerade in kleineren Ämtern immer wieder zurückgestellt werden. Eine Vielzahl von privaten und öffentlich-rechtlichen IT-Dienstleistern bietet der Verwaltung an, solche Lücken zu schließen, etwa durch Cloud-Dienste oder die Nutzung von Rechenzentren. Dadurch können Verwaltungen zwar Kosten sparen, zugleich müssen aber staatliche Daten möglicherweise an private IT-Dienstleister übertragen werden.
Dies wirft eine grundsätzliche Frage auf: Wann ist es Trägern staatlicher Gewalt erlaubt, Daten aus ihrem alleinigen, öffentlich-rechtlich geprägten Einflussbereich zu entlassen und stattdessen einem Privaten einen zumindest mittelbaren Zugriff auf diese zu ermöglichen? Eine Annäherung an diese Frage ermöglicht der Grundsatz der digitalen Souveränität. Dieser kann in bestimmten Konstellationen dazu führen, dass staatliche Daten nicht an private IT-Dienstleister übertragen werden dürfen. Zur Begründung dieses Grundsatzes ergänzen sich drei Überlegungen: der Charakter zwingender Staatsaufgaben, eine staatliche Gewährleistungsverantwortung und das Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen und Institutionen.

Datenverarbeitung selten zwingende Staatsaufgabe

Einen abschließenden Katalog von Aufgaben, die zwingend vom Staat wahrzunehmen sind, enthält die Verfassung nicht. Gleichwohl herrscht darüber Einigkeit, dass manche Aufgaben, wie etwa Gesetzgebung, Justiz oder Strafverfolgung, grundlegende staatliche Funktionen repräsentieren und als solche vom Staat ausgeführt werden müssen. Die Verarbeitung von Daten ist jedoch kaum einmal als zwingende Staatsaufgabe einzuordnen, weil ihre Erhebung und Verwaltung in aller Regel kein Selbstzweck ist, sondern faktisch nur die Erledigung einer anderen spezifischen Aufgabe unterstützt. Doch es gibt Ausnahmen wie zum Beispiel im Meldewesen. Dort ist die Datenverarbeitung selbst unmittelbarer Gegenstand der eigenständigen und primär zu erfüllenden staatlichen Aufgabe.

Staat bleibt in der Verantwortung

Solche Fälle dürften jedoch selten sein. Die Auslagerung der Datenverarbeitung an private IT-Dienstleister ist aber auch dann unzulässig, wenn die betroffenen Daten zwar nicht selbst Gegenstand, wohl aber integraler Bestandteil der zwingenden Staatsaufgabe sind. Die Aufgabenwahrnehmung steht und fällt mit den betreffenden Daten. Je zentraler ein Datenbestand für die Wahrnehmung einer obligatorischen Staatsaufgabe ist, desto weniger kommt eine Privatisierung in Betracht. Dabei ist es weniger entscheidend, dass die Daten erst durch die derzeitige Verfügbarkeit von Informationstechnologien Bedeutung gewonnen haben, sondern seit jeher und traditionell ein elementarer Bestandteil der Aufgabenwahrnehmung gewesen sind; ein Beispiel könnte das Führen von Prozessakten durch die

Zivilgerichte sein.
Daneben kann der Einbindung privater IT-Dienstleister die staatliche Gewährleistungsverantwortung entgegenstehen. Wenn der Staat Private in die Aufgabenwahrnehmung einbezieht, trifft ihn weiterhin die Verantwortung, die ordnungsgemäße und gemeinwohlverträgliche Aufgabenerfüllung durch den Privaten zu gewährleisten. Dabei stellt sich in der Praxis insbesondere die Frage, wie eine effektive Lenkung und Kontrolle der privaten Akteure sichergestellt werden können. Im Zweifel muss der Staat für den Fall des Scheiterns des Privatsektors in der Lage sein, die Aufgabe zurückzuholen und wieder selbst wahrzunehmen.

Vielfältige Risiken

Insofern sind beim Einbinden privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung vielfältige Risiken zu berücksichtigen. Staatliche Daten müssen jederzeit verfügbar sein, dürfen inhaltlich nicht verfälscht, nicht sachfremd durch Dritte genutzt und nicht unbefugt veröffentlicht werden. Es kann nicht pauschal unterstellt werden, dass sich Private eher rechtswidrig verhalten. Doch für IT-Dienstleister in staatlicher Hand ergibt sich eine unmittelbare Grundrechts- und Gesetzesbindung, während private IT-Dienstleister privatautonom gesetzte Ziele verfolgen. Mitarbeiter privater IT-Dienstleister sind grundsätzlich nicht denselben Strafandrohungen ausgesetzt wie Amtsträger (vgl. §§ 203, 11 StGB). Außerdem ist zu berücksichtigen, dass einzelnen privaten IT-Unternehmen eine erhebliche Marktmacht zukommt und in der öffentlichen Verwaltung notwendige IT-Fähigkeiten und -Kenntnisse teilweise noch unterentwickelt sind. Bei Vertragsverhandlungen können deshalb erhebliche Informationsasymmetrien zulasten der öffentlichen Gewalt bestehen. Und es gibt weitere Unterschiede: Private IT-Dienstleister können einem spürbaren Kostendruck ausgesetzt sein. IT-Dienstleister in öffentlicher Hand hingegen sind vom Staat getragen und finanziert und dienen typischerweise nicht der Gewinnerzielung. Während gegenüber IT-Dienstleistern in öffentlicher Hand vielfältige Aufsichts- und Einflussmöglichkeiten bestehen, fehlen diese bei Unternehmen in privater Hand, und es gibt grundsätzlich keine Möglichkeiten, deren operatives Tagesgeschäft zu beeinflussen.

Verbreitung unumkehrbar

Bestehende Risiken werden durch spezifische Charakteristika von Daten verschärft. Durch die Möglichkeit der digitalen Kopie kann eine einmal vorgenommene Verbreitung oder gar Veröffentlichung faktisch kaum mehr rückgängig gemacht werden. Während grundsätzlich bei öffentlichen Aufgaben, zum Beispiel dem Betrieb einer Autobahn, die Kontrolle zumindest ex-nunc wiedererlangt, Fehler korrigiert und ein ordnungsgemäßer Zustand wiederhergestellt werden können, sind beim Umgang mit Daten strukturbedingt negative Folgen denkbar, die sich unumkehrbar in die Zukunft erstrecken. Je nach Umständen des Einzelfalls ist deshalb zu berücksichtigen, ob die Modalitäten der Einbindung Privater und deren Organisationsstruktur ausreichen, um einer staatlichen Gewährleistungsverantwortung gerecht zu werden, entweder zum Schutz der Funktionsfähigkeit der Verwaltung oder im Hinblick auf die Rechtspositionen Dritter.

Eine Frage des Vertrauens

Der Grundsatz digitaler Souveränität wird schließlich durch das Vertrauen in die Integrität und Funktionsfähigkeit staatlicher Strukturen unterstützt. Diesem Gedanken liegen zwei gegensätzliche Entwicklungen zugrunde: Einerseits bedarf es eines erhöhten Vertrauens aufgrund des Einsatzes relativ neu entstandener Informationstechnologien, andererseits entwickelt sich ein Verlust herkömmlicher Kontrollmechanismen. Bislang wurzelte das Vertrauen, das Trägern öffentlicher Gewalt entgegengebracht

wurde, in erster Linie in der Person der einzelnen Amtsträger. Dieser persönliche Aspekt wird durch den Einsatz von Informationstechnologien mehr und mehr in den Hintergrund gedrängt, was wiederum das Bedürfnis nach Vertrauen erhöht. Zugleich wird staatlicher Umgang mit Daten weniger kontrollierbar, weil sich dieser – anders als traditionelles staatliches Handeln – grundsätzlich nicht unmittelbar in der tatsächlichen oder rechtlichen Ordnung auswirkt und als solches auch nicht unmittelbar wahrnehmbar ist. Da eine nachgelagerte rechtliche Kontrolle beim Umgang mit Daten nur bedingt effektiv möglich ist, muss schon auf einer vorgelagerten Stufe durch rechtliche Regelungen klargestellt werden, dass bestimmte Daten einen öffentlich geprägten Herrschaftsbereich gar nicht erst verlassen dürfen.

()

Dieser Beitrag ist in der Ausgabe Februar 2020 von Kommune21 im Schwerpunkt Digitale Souveränität erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Cloud Computing, Digitale Souveränität