Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Digitale Souveränität“

bei VITAKO Herbstempfang

Reichstagsgebäude

Clubraum im Reichstagsgebäude, Plenarsaalebene
Platz der Republik 1
11011 Berlin

16. Oktober 2019, 18.30 Uhr – 20.30 Uhr

Es gilt das gesprochene Wort

Sehr geehrter Herr Kühne (Vorstandsvorsitzender VITAK0),

Sehr geehrter Herr Dr. Bizer,

Sehr geehrte Mitglieder des Deutschen Bundestages,

Sehr geehrte Damen und Herren,

I. Dank für die Einladung

Ich nutze heute der **digitalen Souveränität über meinen Terminkalender** und folge gerne Ihrer Einladung.
Ich möchte auch an Ihrem Erfahrungsschatz teilhaben und Impulse für meine Arbeit mitnehmen.

Gespannt bin ich auf die Ausführungen von **Herrn Dr. Bizer von Dataport**, der nach mir spricht und gerade die kommunale Ebene in besonderer Weise im Blick hat.

Als Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister in Deutschland bündelt **VITAKO** durch den ständigen Austausch von Erfahrungen, Kompetenzen und Strategien fachliche Kompetenz und eine umfassende Übersicht.

VIKAKO weiß daher wie bescheiden es tatsächlich um die digitale Infrastruktur vor Ort bestellt ist.

Sie sind daher ein wichtiger Ansprechpartner für alle, die sich mit dem Einsatz von Informationstechnologie im kommunalen Sektor befassen, ob Behördenleitungen oder Parlamente.

Das gilt selbstverständlich auch für den Datenschutz.

II. Datenschätze in Hülle und Fülle

Sie haben mich um Anmerkungen zum Thema Digitale Souveränität gebeten.

Die digitale Datenlandschaft ist mittlerweile zum Gebirge geworden. Ein Gebirge aus weit mehr als fünf Milliarden Terabyte bzw. fünf Zettabyte an Daten. Bis zum Jahr 2020 wird ein Anwachsen auf 20 bis 40 Zettabyte vorherbesagt. Die Geschwindigkeit des Wachstums ist also ungebremst.

Diese Daten bilden die Grundlage für wichtige Konzepte, beispielsweise der Industrie 4.0, Steuerung von Prozessen sowie allen Arten privater und staatlicher Dienstleistungen. Massenproduktion, Steuerung von komplexen Prozessen und individuelle Anpassung sollen zeitgleich möglich sein. Das ist eigentlich eine gute und wirtschaftlich Erfolg versprechende Strategie.

Es wird aber immer dann heikel, wenn besonders sensible personenbezogene Daten im Spiel sind.

- Gesundheitsdaten aus ***Wearables*** können für neuartige Versicherungstarife genutzt werden.
- Aussagekräftige Sozialprofile basierend auf den bei der Internetnutzung „gewonnen“ Daten dienen als Grundlage für effektivere personenbezogene Werbung und Verhaltensbeeinflussung.
- Die Unbeobachtetheit als unabdingbare Grundlage einer freien, liberalen und pluralen Gesellschaft ist hochgradig gefährdet.

III. Datensouveränität vs. Datenschutz?

Bei der Betrachtung des Begriffs der **digitalen Souveränität** muss man durchaus differenzieren. So vage er ist, so vielfältig wird er von vielen verwendet.

Das Verständnis von digitaler Souveränität, wie es oft seitens der Bundesregierung kommuniziert wird, basiert – ähnlich wie im Urheberrecht – auf dem Gedanken, dass personenbezogene Daten im digitalen Zeitalter auch einen wirtschaftlichen Wert haben. Dieser wirtschaftliche Wert soll dann letztlich (auch) demjenigen zugutekommen, von dem die Daten stammen.

Jeder Bürger und jede Bürgerin sollen nach dieser Idee frei darüber entscheiden dürfen, wie viele seiner Daten, ob sensibel oder nicht, er wem überlassen möchte und vor allem, welchen Preis er dafür verlangt.

Genügt aber ein ökonomisch geprägter Begriff „Datensouveränität“ für die Klärung relevanter Fragestellen?

- Zum Beispiel bei der Problemstellung, ob beispielsweise die Bewertung eines individuellen Falls ausschließlich anhand einer statistischen Auswertung einer großen Gruppe zulässig ist oder nicht?

- Wie sieht es aus bei der **Zweit- oder Drittnutzung** persönlicher Daten bzw. daraus abgeleiteter Erkenntnisse durch Partnerunternehmen, Branchendatenbanken oder Data-Broker aus? Dabei spielt es doch keine Rolle, ob es sich um freiwillig verkaufte Vertragsdaten oder freiwillig veröffentliche Informationen auf sozialen Plattformen handelt. Gerade diese Formen der Verarbeitung werden im Laufe der Zeit immer mehr an Bedeutung gewinnen.

Das **hoch gewinnbringende Big-Data-Konzept** basiert darauf, eben jene unüberschaubar große Anzahl an Daten zusammenzuführen, um sie dann gewinnbringend analysieren zu können. Daten, deren Verkauf und Weiterverarbeitung einzeln betrachtet auf den ersten Blick harmlos erscheinen, könnten dann unvorhergesehene und für die Betroffenen nachteilige Rückschlüsse ermöglichen. Quellen von Journalisten könnten offengelegt oder die Tagesabläufe besonders gefährdeter Personen nachverfolgt werden.

Auf den ersten Blick liegt die Ökonomisierung des Umgangs mit persönlichen Daten durchaus nahe. Allerdings fällt der Anteil des Einzelnen am Schatz der Datensouveränität doch überraschend gering aus. Der Verkauf des eigenen Surf- und Einkaufsverhaltens an professionelle Datenhändler bringt in den meisten Fällen weniger als acht Euro im Monat ein und als Teil eines heutzutage üblicherweise gehandelten Datenpakets fällt der Wert bereits auf einen mageren Cent.

An dem dahinter liegenden Verknüpfungs- und Wertschöpfungsprozess ist der viel beschworene Daten-souverän meist nicht beteiligt und geht entsprechend leer aus.

Zudem muss berücksichtigt werden, dass die vermeintlichen Reize der finanziellen Kompensation für ein auf den ersten Blick unerschöpfliches Gut schnell zu einer „Transparenzoffensive“ vieler Bürgerinnen und Bürger führen könnte. Die Daten verbrauchen sich ja nicht. Sie können theoretisch immer wieder frisch zur Verfügung gestellt werden, um neue Einnahmen zu generieren.

Die technische und ökonomischen Fachkenntnisse, abschätzen zu können, welche Risiken damit einhergehen, die sich unter dem Strich nicht nur aus datenschutzrechtlicher Sicht, sondern sogar finanziell für die Betroffenen auswirken können, werden nicht viele haben.

Am Ende steht einer kleinen Einmalzahlung für die Datenpreisgabe aber vielleicht monatliche Mehrausgaben in größerer Höhe entgegen. Merausgaben, weil basierend auf den – auch bei anderen Gelegenheiten bereitgestellten Daten – z.B. der Algorithmus einer Versicherung den Betroffenen in eine höhere Risikogruppe einsortiert hat.

Insofern greift eine rein ökonomisch ausgerichtete Konzeption der digitalen Souveränität deutlich zu kurz.

Andere Beispiele könnte man noch aus dem Bereich der Plattformen u.ä.m. bringen.

Allen gleich ist die Erkenntnis, dass Datensouveränität oder der oft begleitende „risikobasierte Ansatz“ zum Schutz von Grundrechten und Interessen der Verbraucher nicht ausreichen.

IV. Wer ist souverän, der Staat, die Wirtschaft oder der Betroffene?

Digitale Souveränität wird aber auch noch in einem anderen Kontext verwendet: Anfang des Jahres hat VITKO zu meiner großen Freude in einer Veröffentlichung das faktische Monopol von Microsoft bei den aktuellen Softwareprogrammen in der öffentlichen Verwaltung beklagt. Der amerikanische IT-Gigant herrscht mit seinen Betriebssystemen auch in den Verwaltungen von Bund, Ländern und Gemeinden.

Diskussionsbedarf habe ich bei einer Aussage, dass sich die kommunalen IT-Dienstleister Sorgen machen um **Datensouveränität besonders hinsichtlich aktueller Softwareprodukte von Microsoft.** In der Sache selbst ist die Besorgnis völlig berechtigt. Aber wer ist hier der Träger der Datensouveränität, die er dem Internetriesen gegenüber geltend machen will?

Das passt auch zu einer Äußerung des EU-Kommissars für Digitale Wirtschaft, **Günter Öttinger:** „*Wir haben derzeit keine europäische, keine deutsche, keine eigene digitale Souveränität und zu wenig digitale Autorität. Die zu gewinnen, muss ein Ehrgeiz Europas sein ... Und wir bieten seitens der Europäischen Kommission an, das Ganze zu koordinieren, zu moderieren und zu erreichen, dass Europa ... aus dem Tiefschlaf erweckt wird ..., um Wertschöpfung bei uns zu halten, zurückzukehren zu einer digitalen Souveränität und stärkerer digitaler Autorität.“*

Den bunten Strauß der begrifflichen Möglichkeiten bereichert auch der **Bundesinnenminister.** Er kündigt Gespräche mit Software-Anbietern mit den Worten an: „*Um unsere digitale Souveränität zu gewährleisten, wollen wir Abhängigkeiten zu einzelnen IT-Anbietern verringern.“* Hier wird digitale Souveränität als Unabhängigkeit von allzu mächtigen US-Konzernen verstanden.

Wer ist denn nun Träger der neuen Souveränität?

- der Betroffene i. S. der Datenschutzgrundverordnung?
- der föderale Staat in seinen Gliederungen?
- oder gar die Europäische Union bei ihrem Versuch, sich von der Vorherrschaft der US-Softwareriesen zu lösen?

V. Datenschutz durchsetzen – Individuelle Rechte in der digitalen Welt bewahren

Wir müssen angesichts der Bandbreite der Begriffsbestimmungen aufpassen, dass uns die „Digitale Souveränität“ nicht unter der Hand zerbröselt und ihre normative Verbindlichkeit verliert.

Ich setzte mich für einen Datenschutz ein, der die Bewahrung der Rechte der Menschen in der digitalen Welt in den Mittelpunkt stellt. Niemand darf zum Objekt einer Entwicklung werden, auf die er weder politisch als Teil einer Gemeinschaft noch als individueller Grundrechtsträger wirkungsvoll Einfluss nehmen kann.

Digitalisierung darf deshalb niemals zum Selbstzweck werden.

Dazu brauchen wir eine breite gesellschaftliche Wertedebatte und in Folge klare Gestaltungs- und auch Regulierungsvorgaben. **Datenschutz muss deswegen Kernelement der Digitalisierung sein und schon im Rahmen der Produktentwicklung mitsteuern**.

Das schafft er aber nicht auf nationaler Ebene. Erforderlich ist vielmehr ein europäisches Modell der Digitalisierung. In Frankreich hat man sich z.B. dazu entschieden, einen auf Open-Source basierenden Messengerdienst für die öffentliche Verwaltung zu entwickeln um eine sichere datenschutzkonforme Alternative zu gewerblichen Anbietern wie z.B. WhatsApp zu besitzen. Dieser Dienst soll dann auch für die Bevölkerung freigegeben werden, um mit staatlichen Institutionen (und untereinander) zu kommunizieren.

Warum schließen wir uns dieser Idee nicht einfach in Deutschland an? Wenn dann noch ein paar weitere Staaten mitziehen, kann es schnell passieren, dass dieser Messenger kurz- bis mittelfristig auf den Handys von Millionen Europäern installiert ist. Hier liegt eine echte Chance, eine datenschutzfreundliche Alternative zu vielen kommerziellen Angeboten zu schaffen, die auch von der Verbreitung her eine Chance hat.

VI. Wie „Digitalen Souveränität“ ausgestalten?

Was sind die inhaltlichen Voraussetzungen für einen effektiven Datenschutz? Grundlagen sind und bleiben die informationellen Selbstbestimmung des Grundgesetzes, und die europarechtlichen Grundrechtsgarantien. Grundrechtecharta und weitere Regelungen geben jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht, auf das die **Europäische Datenschutz-Grundverordnung** aufbaut.

Wir haben hier zugleich die tragenden Voraussetzungen dafür, dass zusätzlich so etwas wie Datensouveränität überhaupt Wirksamkeit entfalten kann, ohne den eigentlichen Grundrechtsschutz in die zweite Reihe zu schieben.

Der Fokus muss darauf liegen, die Chancen der Digitalen Souveränität für das Recht auf informationelle Selbstbestimmung herauszuarbeiten und dabei zugleich die Grenzen und Risiken aufzuzeigen.

Begreifen wir **digitale Souveränität** als Stärkung der Verfügungsgewalt des Einzelnen über „seine“ Daten, kann ich mit dem Begriff durchaus leben. Das ist immer dann der Fall, wenn die Souveränität ein **zusätzliches Mittel** ist, das die Autonomie des Einzelnen auch in einem wirtschaftlichen Sinne stärkt.

Sofern also der Einzelne frei darüber entscheiden kann, was mit seinen Daten passiert, ist es richtig, ihn auch an dem wirtschaftlichen Wert seiner Daten teilhaben zu lassen.

Wenn der Einzelne dann tatsächlich souveräner mit seinen Daten umgeht und sich besser um den Umgang „kümmert“, kann ich das nur begrüßen.

Unverzichtbar ist, dass der Gedanke der Souveränität zusätzlich, gewissermaßen als Ergänzung zum Recht auf informationelle Selbstbestimmung betrachtet wird. Es muss klar sein, dass Recht auf informationelle Selbstbestimmung ein immaterielles Recht, ist, dass auf dem Persönlichkeitsrecht und der Menschenwürde des Einzelnen fußt.

Es ist nicht möglich, den Menschenwürdegehalt außen vor zu lassen. **Die Persönlichkeit als solche ist eben nicht verkäuflich, auch nicht im Austausch mit den vermeintlichen ökonomischen Segnungen der digitalen Souveränität.**

Klar sein muss also, dass digitale Souveränität nur dann ein Gewinn ist, wenn sie zusätzlich zum – immateriellen – Recht auf informationelle Selbstbestimmung verstanden wird.

Ohne definierte und verbindliche Regeln für die digitale Wirtschaft wird es nicht gehen. Sonst bleibt von der erhofften Souveränität wenig übrig. Eine Reduzierung der eigenen Daten auf ein reines Handelsgut missachtet das tiefgreifende menschliche Bedürfnis, sich frei von Beobachtung sicher zu fühlen.

VII: Schlussbemerkung mit Hinweis auf die DSGVO

Ich möchte an dieser Stelle einer richtig verstandenen Digitalen Souveränität durchaus aufgeschlossen gegenübertreten.

Sie darf aber die Stärkung einer selbstbestimmten Inanspruchnahme der informationellen Selbstbestimmung nicht aus den Augen verlieren.

Die Datenschutzgrundverordnung der EU setzt die richtigen Schwerpunkte. Bei digitalen Anwendungen soll der Datenschutz von Anfang an mitbedacht und eingebaut werden. Die DSGVO schafft einen verbindlichen Rahmen für alle Marktteilnehmer gleichermaßen. So erhalten die Bürgerinnen und Bürger überhaupt erst die Möglichkeit, die Nutzung ihrer Daten zu kontrollieren - **und tatsächlich zum Souverän zu werden**.

Auch mit tatkräftiger Unterstützung starker Aufsichtsbehörden können wir auf der Basis des Schutzes personenbezogener Daten

- einen faireren Wettbewerb schaffen,
- einen Wettbewerb, in dem sich die Entwicklung von datenschutzfreundlichen Anwendungen lohnt,
- die einen echten Mehrwert für die Bevölkerung bieten.

In Zukunft wird der Datenschutz mit der Wirtschaftsförderung durch die Schaffung einheitlicher und verbindlicher Standards für den Umgang mit Daten also eine neue Aufgabe bekommen.

Das fundamentale Ziel wird jedoch immer der Schutz des informationellen Selbstbestimmungsrechts sein.

Die Menschen haben zumeist nur dann den Mut, in freier Selbstbestimmung an unserer Gesellschaft mitzuwirken, wenn sie wissen, wer was von ihnen weiß und dass er sich auf den Schutz empfindlicher Daten verlassen kann.

Ich danke für Ihre Aufmerksamkeit