

VATM-Standpunkt zur digitalen Souveränität Europas

Die neue EU-Kommission unter Präsidentin Ursula von der Leyen möchte Europa fit für das digitale Zeitalter machen. Dabei hängt die Umsetzung des digitalen Binnenmarktes und somit die Zukunft der europäischen Wirtschaft entscheidend davon ab, welche unionsinternen Strukturen geschaffen werden und wie sich Europa im internationalen Wettbewerb mit den großen Industriestaaten wie den USA oder China positioniert. Wirtschaftspolitik ist mittlerweile nicht mehr von Digitalpolitik abzugrenzen, da die europäische Wertschöpfung entscheidend von der digitalen Innovationskraft abhängt. In diesem Zusammenhang wird immer wieder von der digitalen Souveränität Europas gesprochen und von der Wichtigkeit einer europäischen Digitalstrategie, um das enorme Potential einer erfolgreichen digitalen Transformation für Europa freizusetzen und die Spielregeln unserer digitalen Zukunft, die derzeit anderswo gemacht werden, aktiv mitzugestalten. Aber Europa zögert: Der Ausbau digitaler Projekte kommt nicht so recht voran und von einer einheitlichen Digitalstrategie ist man weit entfernt. Das gefährdet die Souveränität der europäischen Staaten. Europa ist von US-amerikanischen Unternehmen stark abhängig und läuft China in der digitalen Entwicklung hinterher.

Technologische Souveränität

Digitale Souveränität ist ein schillernder Begriff, der zahlreiche Einzelaspekte von technologischer Kompetenz über Datenverwendung und Nutzungsrechte bis zu zentralen Sicherheitsfragen hinsichtlich solcher Daten aber auch Technologien umfasst. Digitale Souveränität betrifft damit auch Fragen allgemeiner nationaler europäischer und internationaler Wirtschafts- und Sicherheitspolitik und geht weit über die zentralen Interessenbereiche des Verbandes und der TK-Industrie hinaus. Für unseren Bereich sind dennoch Kernbereiche der aktuellen Diskussion für die weitere Entwicklung zukünftiger und bestehender Geschäftsmodelle von allergrößtem Interesse. Besondere Schwerpunkte zu setzen lohnt es daher gerade zum jetzigen Zeitpunkt. Die Fähigkeit, eigenständig Spitzentechnologien zu entwickeln und hierfür möglichst uneingeschränkt und ohne politische Vorgaben über den Einsatz von Partnertechnologien zu entscheiden, erweist sich gerade bei der Implementierung von 5G etwa als besonders bedeutsam. Unbeschadet der absolut notwendigen und nachvollziehbaren Diskussion zu Sicherheitsfragen und unerwünschter Technologieabhängigkeit, muss die Wirtschaft in Europa so weit als möglich in der Lage sein, die Vorteile der Globalisierung und Spezialisierung für die eigene zukunftsfähige Entwicklung zu nutzen und im Wettbewerb im Weltmarkt mit Produkten und Dienstleistungen bestehen zu können.

Digitale Souveränität bedeutet in diesem konkreten Zusammenhang daher nicht nur eigene europäische oder gar nationale Spitzentechnologien selbst zu entwickeln – was unzweifelhaft wichtig ist und verstärkt in den politischen Fokus genommen werden muss – sondern auf der anderen Seite auch weiterhin europäische Spitzen – Dienstleistungen und Spitzen- Technologien anbieten zu können, auch wenn hierzu von weltweit marktführenden Zulieferern Produkte bezogen werden müssen. Weltmarktqualität und Weltmarktpreise wettbewerbsfähig anbieten zu können, gehört absolut gleichwertig in die Diskussion zur digitalen Souveränität eingebracht. Eine politisch abgehobene Diskussion, die sogar wörtlich absolute Sicherheit fordert, Netzebenen und Bauteile mit völlig unterschiedlichen Gefährdungspotentialen unbeachtet lässt und auf diesem Wege eine völlig undifferenzierte Sicherheitsdiskussion führt, schadet der digitalen Souveränität Deutschlands und Europas. So wichtig es ist, die digitale Transformation auch stärker durch die Entwicklung von möglichst eigenen digitalen Produkten voranzutreiben und die Wertschöpfung nicht vollends ins Ausland zu verlieren, so sollte dies nicht bedeuten, protektionistische Maßnahmen zu ergreifen oder Anbieter aufgrund ihres Herkunftslandes oder politischer Strukturen per se zu verbieten.

Multi Vendor Strategien, Transparenz von Quellcodes, harte Sicherheitskontrollen vor und während des Betriebs, Beweislastumkehrelemente und drakonische Sanktionsmöglichkeiten europäisch abgestimmt, würden in vielen Fällen pauschale Verbote und politische Überreaktionen ersetzen und echte digitale Souveränität sicherstellen können.

Grundvoraussetzung für eine zunehmend digitale Wirtschaft, digitale Verwaltung und Digitalisierung der Gesellschaft, Grundvoraussetzung für Wachstum und Wohlstand, ist die Versorgung aller Länder und Regionen mit entsprechenden Infrastrukturen und Diensten. Der Telekommunikationssektor spielt hier eine Schlüsselrolle, da nur der flächendeckende Ausbau mit neuen Gigabit-Kommunikationsnetzen und der Wettbewerb auf diesen Netzen die Innovationen fördern, die Europas Wirtschaft braucht, um im internationalen Wettbewerb bestehen zu können. Europa muss sich dabei auf neue Schlüsseltechnologien wie beispielsweise 5G konzentrieren können – mit bester Qualität und sinnvollen Preisstrukturen. Digitale Souveränität ist zu komplex für zu einfache (Schein-)Lösungen.

Datensouveränität

Wenn wir von digitaler Souveränität sprechen, ist die Datensouveränität zentrales, wenn nicht das Schlüsselement. Aktuell stehen viele Europäer der Digitalisierung und der Fähigkeit des Staates, persönliche Daten zu schützen, eher kritisch gegenüber.

Akzeptanz in der Gesellschaft und damit auch zukünftiges Wirtschaftswachstum sind somit davon abhängig, ob Digitalisierung auf zuverlässigen, sicheren, vertrauenswürdigen und transparenten Technologien beruht. Grundvoraussetzung ist dabei aber nicht nur der Schutz von Bürgerdaten, die Bürger sollen auch eine informierte Entscheidung darüber treffen können, welche Dienste und Funktionen sie nutzen möchten und welcher Art der Datenverarbeitung (Erhebung, Speicherung, Auswertung, Weitergabe, wirtschaftliche Nutzung) sie deshalb zustimmen.

Auch hier ist digitale Souveränität aber nicht eindimensional zu sehen. Wichtige zukünftige und oft KI-basierte Dienste werden sich nur entwickeln können, wenn Daten erhoben und (in anonymisierter Form) ausgewertet werden können. Verkehrssicherheit, Gesundheit etc. mögen an dieser Stelle beliebig erweiterbar genügen. Bestimmte Dienstleistungen werden nur möglich und für den Kunden nutzbar sein, wenn dieser seinerseits Daten hierfür zur Verfügung stellt. Auch hier gilt aber eine größtmögliche Transparenz und Sicherheit – wo gewünscht und erforderlich auch Anonymität. Pauschale Verwertungsverbote sowie das Gebot der Datensparsamkeit in seiner bisherigen Form, werden aber definitiv einer Digitalen Souveränität unserer gesamten Gesellschaft zuwiderlaufen. Unsere nationale wie europäische Wirtschaft wird wie auch unsere zukünftige Gesellschaft auf die Auswertung digitalisierter Daten essentiell angewiesen sein, um den internationalen Entwicklungen Stand halten zu können.

Auch der Schutz von Geschäftsgeheimnissen der Unternehmen, Forschungseinrichtungen, der Daten von Finanzinstituten und staatlichen Einrichtungen ist ein entscheidender Faktor. Hier kommt es aber ebenfalls nicht nur auf die unzweifelhafte Sicherheit von Unternehmensdaten lokal, in Cloudlösungen oder im Mailverkehr an, sondern auch darauf, souverän über Bestand und Migration von Daten bestimmen zu können, etwa beim Wechsel von Anbietern mit oft proprietären Systemen, was heute keinesfalls sichergestellt ist. Eine gravierende Abhängigkeit der Wirtschaft von einzelnen, oft, aber nicht immer marktmächtigen Anbietern, bereitet auch Bundesregierung und Kommission immer größere Sorge.

Zumindest beim Problem Cloudsicherheit scheint Bewegung in die nationale, aber auch europäische Diskussion zu kommen. So setzen sich Telekom und VATM-Mitgliedsunternehmen gleichermaßen für die europäische Cloud GAIA-X ein, bei der die Daten weder in die USA noch nach China gelangen sollen.

Digitale Transformation

Europa ist technologisch ins Hintertreffen geraten. Zu lange wurde veraltete Technik eingesetzt und geschützt. Außerdem wurde leichtfertig in Kauf genommen, dass europäische Innovationen von anderen Industriestaaten aufgekauft werden und somit technisches Knowhow Europa verlässt. Eine vergleichsweise schwache Start up-Kultur und noch viel schlechtere Finanzierungsmöglichkeiten für junge Unternehmen, Bürokratie und stark regulierte Märkte sind nur ein Teil der sehr vielschichtigen Gründe und daher auch nur ein Teil der Herausforderungen vor denen wir stehen, wenn Europa aufholen oder gar eine digitale Vorreiterrolle übernehmen will. Damit sich neue Geschäftsmodelle entwickeln können, muss ein investitionsfreundliches Umfeld geschaffen werden. Die Aufgabe der neuen EU-Kommission ist es, dafür zu sorgen, dass der digitale Binnenmarkt die richtigen Rahmenbedingungen für Innovationen setzt und dabei die europäischen Werte nicht als Hemmschuh, sondern als Wettbewerbsvorteil einzusetzen weiß. Außerdem muss der Infrastrukturausbau in den EU-Mitgliedstaaten stärker unterstützt werden, damit dank Investitions- und Dienstewettbewerb möglichst ähnliche Rahmenbedingungen in allen Regionen Europas geschaffen werden. Der Infrastrukturausbau und damit die digitale Transformation sind ganz wesentlich auch von der Akzeptanz der Bürger abhängig. Statt neuer aber überwiegend ungenutzter neuer Hochleistungsnetze brauchen wir gute Auslastungsquoten – möglichst schon zum Ausbaupunkt, da sich dadurch nicht nur die Wirtschaftlichkeit des Ausbaus massiv verbessert, sondern auch die Basis für unsere Digitalisierung erst geschaffen wird. Zuerst brauchen wir die Henne – und die ist ein Netz mit möglichst vielen Kunden – dann entwickeln sich die digitalen Angebote deutlich schneller. Erst wenn wir eine kritische Masse erreichen lohnen sich solche Dienste oder machen überhaupt erst Sinn. Wie bei den Smartphones werden sich neue Dienste in der Masse erst entwickeln und zum Wirtschaftsfaktor werden, wenn genug Kunden diese nutzen können.

Digitale Souveränität auf Basis völlig neuer digitaler Märkte wird sich in Europa nicht so schnell entwickeln wie in Asien und Amerika, wenn dort neue Mobilfunk und Glasfaserinfrastruktur schneller ausgebaut wird. Nicht Leuchttürme oder ein paar Industrieregionen werden dabei das Spiel bestimmen, sondern die absolut breite Verfügbarkeit auch im ländlichen Raum, wo neben Heimarbeit, Gesundheitsversorgung etc. vor allem der Mittelstand als wichtiger Wirtschaftsfaktor für die Digitalisierung hinzukommt. Eine Nachfrageförderung wie beispielsweise durch ein, wie vom VATM gefordertes Voucher-System, für anschlusswillige Bürger beim Glasfaserausbau ist deshalb gerade für Deutschland essenziell, dient der Digitalisierung und der Digitalen Souveränität unseres Landes.

Ein weiterer, nicht zu vernachlässigender Aspekt sind ausreichend Mittel für Forschung und Entwicklung, Bildung und Förderung einer europäischen Zukunftsstrategie, die sich mit den bereits bestehenden Plänen etwa Chinas auseinandersetzt. Die AI-Alliance der EU-Kommission ist ein erster Schritt in die richtige Richtung. Weitere Initiativen müssen folgen – gemeinsam mit der europäischen Wirtschaft, um die richtigen Impulse für das kommende Jahrzehnt zu setzen. Europäische Wirtschaftskooperationen, in denen gemeinsam Kräfte gebündelt werden, sind daher unerlässlich. Europäische Forschungsgelder müssen auch bei europäischen Unternehmen ankommen, damit europäisches Knowhow geschaffen werden kann. In diesem Kontext darf auch kein technologischer Ausverkauf von europäischen Zukunftstechnologien stattfinden. Europäisch geförderte Projekte müssen in Europa gehalten werden, damit hier erhaltene Patente auch von europäischen Unternehmen genutzt werden können.

Die Zukunft Europas hängt auch von den Fähigkeiten der nächsten Generationen ab. Programmieren, Coden, Gestalten, Konzipieren und vernetztes Denken sind die digitalen „Skills“ für viele Berufe der Zukunft. Diese werden aber in unserem heutigen Bildungssystem kaum angemessen vermittelt. Aufklärungsarbeit über die Gefahren der digitalen Welt und über ihr Potential muss Hand in Hand gehen.

Wettbewerbspolitik und Innovationen

Begriffe wie „Internet of Things“, „Big Data“, „Künstliche Intelligenz“ und „Virtual & Augmented Reality“ definieren die Zukunft gerade auch für den TK-Sektor. Die Telekommunikationspolitik des letzten Jahrzehnts – zumindest im Mobilfunkmarkt – war auf die Absenkung der Endkundenpreise fokussiert. Wir brauchen eine Politik, die zu mehr Investitionen anspornt, nicht aber zu weniger Wettbewerb führt.

In Europa wurden daher mit der Datenschutzgrundverordnung (DSGVO) sowie durch das wer-tebasierte, europäische Wettbewerbsrecht Grundlagen geschaffen, Verbraucher und Unter-nehmen zu schützen.

Allerdings schreitet die digitale Transformation mit großer Geschwindigkeit voran, so dass der bestehende Rechtsrahmen den Herausforderungen der modernen Gesellschaft so nicht mehr gewachsen ist und nicht mehr auf alle Gegebenheiten des europäischen Binnenmarktes rea-gieren kann. Eine Anpassung des Rechtsrahmens ist daher unvermeidbar. Er muss neuen Geschäftsmodellen und Investitionen zu Gute kommen. Unternehmen müssen innovativ den-ken und dabei vom Rechtsrahmen unterstützt und nicht gebremst werden. Dabei brauchen wir ein Level Playing Field mit Unternehmen, die auf den hiesigen Markt drängen, oftmals vom Ausland aus agieren und regulatorisch in wesentlichen Teilen anders behandelt werden, ob-wohl die angebotenen Dienste einstweilen direkt im Wettbewerb zu TK-Unternehmen stehen. Im Zeitalter der „sharing economy“ müssen hier entsprechende Impulse gesetzt werden, um regulatorische Nachteile auszugleichen, damit in Zukunft auch europäische, auf Daten basie-rende Geschäftsmodelle geschaffen werden können.

Die Telekommunikationsanbieter verwahren viele personenbezogene Daten und haben diese bisher gut sichern können. Jedoch verschiebt sich das personenbezogene Datenvolumen von klassischen TK-Diensteanbietern mehr und mehr in Richtung OTTs. An dieser Stelle muss die EU Stärke zeigen. Diejenigen, die solche Daten zu sichern haben, brauchen verlässliche und eindeutige Vorgaben. Solange es keine klaren Regeln für die Sicherung von Daten gibt, wird die bestehende Unsicherheit europäischen Unternehmen und Bürgern gleichermaßen scha-den. Notwendig ist eine harmonisierte Vorgehensweise – nur einheitliche und europaweite Regeln können die Lösung sein. Der ePrivacy-Vorschlag zielte auf diese Problemlage, führt jedoch in der Praxis zu einer Stärkung der Browserbetreiber, indem der zentralen Einstellung zur Einwilligung zum Setzen von Cookies in der Zugangssoftware zum Internet – also dem Browser – eine wesentliche Rolle zugemessen wird. Die Browser-Hersteller drohen im Zuge der geplanten ePrivacy-Verordnung zu mächtigen Gatekeepern der digitalen Welt zu werden. Durch diese, sich rasant ändernde digitale Landschaft, wächst zudem die Rolle digitaler Platt-formen: Google kontrolliert den Markt für Suche und mobile OS, Amazon kontrolliert den Markt für Online-Shopping und Facebook kontrolliert den Markt für soziale Netzwerke. Obwohl Eu-ropa den Ton und die Standards in der Telekommunikation und im Datenschutz vorgibt, fehlt es an digitaler Innovation. Dies zeigt sich daran, dass es kein bedeutendes europäisches Be-triebssystem, keinen Browser, kein soziales Mediennetz-

werk, keinen Nachrichtendienst und keine Suchmaschine gibt. Außerdem sind digitale IDs im Datenzeitalter von essenzieller Bedeutung und fast kein Dienst ist ohne Identifizierung mehr nutzbar. Denkt man an die heutigen Dienste (E-Mail, Social Media und Kommunikationsdienste, Online-Shopping, Online-Banking, Zugang zu verschiedenen Formen von Inhalten), so wird deutlich, dass digitale IDs zur Grundvoraussetzung für eine digitale Existenz in Wirtschaft und Gesellschaft geworden sind. Diese Bedeutung wird sich auch bei zukünftigen Diensten (Mobilität, Smart Home, IoT-Anwendungen, eGovernment-Dienste) fortsetzen. Alle Dienste benötigen IDs – und diese Entwicklung betrifft alle Branchen. Von daher freuen sich viele Nutzer, dass es immer häufiger die Möglichkeit gibt, sich mittels eines Facebook-Kontos oder eines Google-Accounts in andere Dienste einzuloggen: Das Konto wird so zu einer Art Generalschlüssel – und man muss sich nur noch ein Passwort merken. Die Kehrseite: Die US-Konzerne werden weiterhin gestärkt, erfahren viel über die Nutzer: wo sie sich einloggen, wie lange sie dort sind – für Google und Facebook sozusagen Gold wert Informationen, denn je besser sie den Nutzer kennen, umso besser können sie zielgruppengenaue Werbung verkaufen.

Das Ziel ist klar definiert: Aufbau eines europäischen Digital Identity Ökosystems für eine sichere Online-Identifikation und Altersverifikation, das nur die für den entsprechenden Dienst notwendigen personenbezogenen Daten verlangt. Digitale Identitäten von offiziellen Stellen sowie von kommerziellen Akteuren, die im europäischen Binnenmarkt tätig sind, sollen dafür nutzbar sein. Es gibt in Europa bereits offene ID-Standards, die einen offenen Ansatz gegenüber den geschlossenen Ökosystemen von Google, Facebook und Apple bieten: Die Industrie startet Initiativen wie die europäische netID, die es jedem Unternehmen ermöglicht, seinen Nutzern die Möglichkeit zu geben, die ID/den Account, die es bei dem Unternehmen hat, auch über andere Plattformen zu nutzen. Diese sollten in geeigneter Weise durch die EU unterstützt werden. Die neue Kommission hat bereits mit der Arbeit an der künftigen Regulierung digitaler Dienste begonnen. Der angekündigte Digital Services Act will die notwendige Vereinheitlichung des Rechtsrahmens verstärken, um die europäische digitale Wirtschaft zu fördern. Dort könnten die neuen Anforderungen für die Integration einer offenen europäischen ID verankert werden.

Zusammenfassung und Forderungen

Digitale Souveränität beinhaltet zahlreiche Komponenten: Sicherheit von Technologien aus Drittländern, aber auch Nutzbarkeit und der selbstbestimmte Einsatz von hochwertigen Technologiebausteinen zur Entwicklung eigener Technologien und Dienste – insbesondere auch im Rahmen der neuen 5G-Welt – sind Ausdruck differenziert verstandener digitaler Souveränität. Datensicherheit und Datensouveränität für Bürger und Unternehmen ist ebenso Ausdruck digitaler Souveränität wie auch die Nutzung möglichst vieler Daten zur Entwicklung digitaler Dienste, die in Verbindung mit KI eine zentrale Rolle in den zukünftigen Wertschöpfungsketten spielen werden. Sichere Cloudlösungen werden unabdingbare Voraussetzung für das Vertrauen der Wirtschaft und Wachstum in Europa sein. Bei der Digitalen Transformation gilt es erhebliche Wettbewerbsverwerfungen zu Lasten des europäischen Industriestandortes bestmöglich auszugleichen und einen rechtlichen Rahmen zu finden, der OTTs und großen nicht europäischen Plattformbetreibern nicht immer größere Vorteile verschafft. Die Datenschutzgrundverordnung (DSGVO) sowie das europäische Wettbewerbsrecht müssen angepasst werden und Digitalisierung, Datennutzung sowie neue europäische Plattformentwicklung erleichtern.

Der VATM formuliert dahingehend folgende Forderungen, damit Europa eine Vorreiterrolle im Digitalbereich einnehmen und seine digitale Souveränität garantieren kann:

1. Digitale Souveränität darf kein nationaler Alleingang sein: wir brauchen gemeinsame europäische Strategien, die den zahlreichen Aspekten und Herausforderungen bei der digitalen Transformation gerecht werden.
2. Die Versorgung der Verbraucher und Unternehmen mit schnellem Internet, vor allem aber die tatsächliche Nutzung der Netze verstärkt durch eine nachfrageseitige Förderung ist essenziell für die digitale Transformation.
3. Wir brauchen eine deutlich verstärkte Förderung europäischer Technologien und Sicherheitskonzepte insbesondere auch von europäischen Cloudlösungen wie GAIA-X.
4. Die Offenheit für Zuliefermärkte mit Hochtechnologie muss gewährleistet bleiben, damit europäische Unternehmen im Wettbewerb bestehen können.
5. Wir brauchen neue Sicherheitskonzepte und Sanktionen zu deren Durchsetzung, wo immer dies zum Schutz der digitalen Souveränität erforderlich ist.
6. Datenschutz und Datensicherheit müssen so an die neuen Herausforderungen der Digitalisierung angepasst werden, dass gleichwohl KI und datenbasierte neue digitale Dienste ermöglicht werden.

7. Das europäische Wettbewerbsrecht muss an die neuen Marktgegebenheiten angepasst werden, es muss ein Level Playing Field mit außereuropäischen Unternehmen, die auf den hiesigen Markt drängen, geschaffen werden.
8. Die obligatorische Einführung eines offenen europäischen ID-Logins ist unerlässlich und könnte die Abhängigkeit von den sich ausbreitenden Login-Diensten der GAFAs (Google ID, Facebook ID, Apple ID) verringern.
9. Förderung von Forschung und Entwicklung muss europäischen Kooperationen zu Gute kommen.
10. Digitale Bildung muss frühzeitig das Wissen, welches für eine digitale Welt von morgen benötigt wird, vermitteln.

Brüssel, den 20.01.2020