Positionspapier

Digitale Souveränität Europas fördern

25. März 2021

Tobias Tenner
Associate Director
Leiter Digitalisierung
Telefon: +49 30 1663-2323
tobias.tenner@bdb.de

Simon Zieglgruber
Associate
Telefon: +49 30 1663-2327
simon.zieglgruber@bdb.de

Bundesverband deutscher Banken e. V.
Burgstraße 28
10178 Berlin
Telefon: +49 30 1663-0
Telefax: +49 30 1663-1399
www.bankenverband.de
USt.-IdNr. DE201591882

Inhalt

1 Executive Summary

Die digitale Souveränität Europas ist eine Grundvoraussetzung dafür, dass die europäische Wirtschaft ihre Innovations- und damit Wettbewerbsfähigkeit auch mittel- bis langfristig beibehalten kann. Bislang ist diese Souveränität nur in sehr eingeschränktem Maße Realität: Die zunehmende Konzentration wirtschaftlicher Macht und technologischen Know-hows bei großen, nicht-europäischen Online-Plattformen hat dazu geführt, dass diese als Gatekeeper, insbesondere der digitalen Wirtschaft, operieren können. Gleichzeitig agieren jedoch auch deutsche und europäische Unternehmen stark vernetzt in einer globalisierten und dadurch hochgradig arbeitsteiligen Welt. Eine vollständige digitale Souveränität im Sinne einer Abschottung ist vor diesem Hintergrund daher nicht wünschenswert. Das vorliegende Positionspapier soll das Bewusstsein dafür wecken, dass ein Balanceakt notwendig ist, um einerseits die digitale Souveränität Europas zu stärken, andererseits an einer offenen und flexiblen europäischen Wirtschaft in einer globalisierten Welt festzuhalten. Protektionistische Maßnahmen, die darauf abzielen, digitale Souveränität zu verwirklichen, haben negative Auswirkungen auf den Standort Europa und müssen daher vermieden werden.

Um die digitale Souveränität Europas und im speziellen der Finanzindustrie zu stärken, sind im vorliegenden Positionspapier im Sinne der vier Souveränitätsdimensionen – Infrastruktur-, Daten-, Entscheidungs- und Plattformsouveränität – konkrete Forderungen der Finanzindustrie herausgearbeitet:

- Überarbeitung der bestehenden wettbewerbsrechtlichen Rahmenbedingungen zu einem modernen Wettbewerbsrecht, das faire Bedingung im digitalen Wettbewerb schafft
- Förderung von Cloud Banking in Europa durch Abschaffung regulatorischer Hürden und Schaffung europäischer Standards, um eine Flexibilisierung und Leistungssteigerung der IT-Infrastruktur zu ermöglichen
- Unterstützung der Datenökonomie durch Schaffung eines branchenübergreifenden Datenrahmens, um datengetriebene Wertschöpfung in allen Industrien und zum Nutzen der Kunden zu ermöglichen
- Aufbau und Ausbau der Kompetenzen im Bereich Cybersicherheit, um nicht nur kritische Infrastrukturen zu schützen, sondern insbesondere Vertrauen des Einzelnen in die digitale Wirtschaft zu stärken
- Fokussierung auf ein mehrstufiges Vorgehen zur Einführung eines programmierbaren Euros, um insbesondere deutsche Industrieunternehmen bei der digitalen Transformation zu unterstützen
- Schaffung eines europäischen digitalen eID-Ökosystems

Alle Anstrengungen zur Stärkung der digitalen Souveränität sollten zum Ziel haben, einen gemeinsamen europäischen Weg zu gehen. Diesem europäischen Weg müssen Werte und Standards wie Vertrauen, Offenheit, hoher Datenschutz und eine kluge Governance zugrunde liegen bei gleichzeitigem Erhalt der Wettbewerbsfähigkeit europäischer Unternehmen.

2 Wie viel digitale Souveränität braucht Europa?

„Europa muss seine digitale Souveränität stärken" – mit diesem Appell haben sich Anfang März 2021 vier europäische Regierungschefinnen, darunter Bundeskanzlerin Angela Merkel, an die Europäische Kommission gewandt und einen Aktionsplan für mehr digitale Souveränität gefordert. Dieser jüngste Vorstoß unterstreicht noch einmal, welche Bedeutung dieses Thema in den letzten Jahren erlangt hat. In kaum einer politischen Debatte über Europas Rolle in der Welt fehlt die Forderung nach digitaler Souveränität; der Begriff ist inzwischen zu einem Synonym für die europäische Aufholjagd im globalen Wettrennen um die technologische Führerschaft, insbesondere mit den USA und China, geworden. Doch ist damit noch nicht definiert, was digitale Souveränität alles umfassen soll. Auf dem letzten Digitalgipfel der Bundesregierung Ende 2020 hat Bundeskanzlerin Angela Merkel es so formuliert: „Europa muss im Prinzip alles können" – mit anderen Worten, Europa muss ohne Einschränkungen unabhängig sein. Die Staatsministerin für Digitalisierung, Dorothee Bär, hat demgegenüber etwas eingeschränkt: „Digitale Souveränität heißt für mich, dass wir in der Digitalisierung unseren eigenen, europäischen Weg gehen und die digitale Transformation (…) selbstbestimmt gestalten wollen. Es geht weder (…) darum, alles in Europa selbst zu machen. Es geht darum, souverän zu entscheiden, in welchen Bereichen wir unabhängig sein wollen und wo wir dafür investieren müssen."

Im Kontext der politischen Diskussion darüber, wie die Wettbewerbsfähigkeit von Banken und FinTechs in Europa gesichert werden kann, hat die Debatte zur digitalen Souveränität bereits ihren Niederschlag in der Regulierung des europäischen Finanzsektors gefunden. Legislative Initiativen wie DORA und MiCA, DSA und DMA zeigen die Bemühungen der Politik, die digitale Souveränität des europäischen Wirtschaftsstandortes und Finanzplatzes zu stärken. Aber auch die von der Bundesregierung initiierte europäische Initiative GAIA-X für eine offene Dateninfrastruktur weist in diese Richtung. Und dennoch liegt ein langer Weg vor Europa, wenn es seine digitale Souveränität sichern will. Einige Daten und Zahlen verdeutlichen dies: So arbeitet China bereits seit 2015 an einer digitalen Zentralbankwährung, Google beherrscht fast den gesamten europäischen Markt für Suchmaschinen und die überwiegende Mehrheit der europäischen Internetnutzer ist täglich auf Facebook aktiv – zusammen mit seinen beiden weiteren Diensten WhatsApp und Instagram ist der Facebook-Konzern schon heute ein kaum noch wegzudenkender Bestandteil des Lebens vieler Europäer.

Entscheidend wird sein, die digitale Souveränität Europas zu stärken und zugleich sicherzustellen, dass offene und flexible Wirtschaftsaktivitäten in einer globalisierten Welt nicht gefährdet werden. Das Ziel, technologische Selbstbestimmung zurückzuerobern, darf nicht ausblenden, dass wir in einer vernetzten Welt leben und von dieser vernetzten Welt profitieren. Mit anderen Worten: In einer globalisierten und dadurch hochgradig arbeitsteiligen Welt wird eine vollständige digitale Souveränität nicht erreichbar sein; ein Balanceakt ist notwendig. Im Folgenden zeigen wir daher Wege zu einer ausbalancierten digitalen Souveränität Europas auf und stellen zugleich die spezifisch auf den Finanzsektor bezogenen Forderungen des Bankenverbands vor, die sich diesem Ziel verschreiben.

3 Was macht digitale Souveränität aus?

3.1 Entstehung des Begriffs

Mit dem Begriff der digitalen Souveränität hat sich in jüngster Zeit der Anspruch herausgebildet, europäische Führung und strategische Autonomie im digitalen Bereich zu erlangen. Der Begriff beschreibt damit die Fähigkeit Europas, in der digitalen Welt unabhängig handeln zu können und dabei sowohl Schutzmechanismen einzusetzen als auch offensive Instrumente zur Förderung digitaler Innovationen.

Ein Bericht der Europäischen Kommission zur Mediensouveränität (von März 2019)[1] hebt hervor, dass die Macht der globalen Technologieunternehmen, die das Sammeln und die Analyse von Daten in den Mittelpunkt ihrer Strategie stellen und sich dabei nicht immer an europäischen Regeln und Grundwerten orientieren, eine große politische Herausforderung für Europa darstellt. Zudem hatte das Europäische Parlament 2019 tiefe Besorgnis über die Sicherheitsbedrohungen geäußert, die mit der wachsenden technologischen Präsenz Chinas in der EU verbunden sind, und mögliche Maßnahmen auf EU-Ebene gefordert, um die Abhängigkeit Europas zu verringern.

Was konkret bedeutet dies für das Konzept „digitale Souveränität"? Welche Bereiche müssen definiert und welches Kompetenz- und Autonomieniveau sollte erreicht sein, damit von digitaler Souveränität die Rede sein kann? Die Bertelsmann-Stiftung hat im Sommer 2020 in einem Beitrag festgestellt, dass „digitale Souveränität" unterschiedlich definiert wird, und selbst einen Definitionsversuch unternommen:

> „Digitale Souveränität ist die Fähigkeit einer Entität, über die zukünftige Ausgestaltung festgestellter Abhängigkeiten in der Digitalisierung selbst entscheiden zu können und über die hierfür notwendigen Befugnisse zu verfügen."[2]

Aus unserer Sicht ist wichtig, dass digitale Souveränität im Sinne einer eigenen Entscheidungs- und Handlungsfähigkeit nicht nur auf einer Analyse der Gegenwart basieren darf. In die Erwägung darüber, als wie kritisch und unverzichtbar eine Dienstleistung, ein Produkt oder eine Branche eingestuft werden, müssen auch zukünftige Entwicklungen und der globale Gesamtkontext miteinfließen.

[1] https://ec.europa.eu/info/sites/info/files/guillaume_klossa_report_final.pdf, abgerufen am 10.03.2021

[2] https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Souveraenitaet_in_der_EU_Policy_Brief_BSt_EZ_European_Public_Goods_DE.pdf, abgerufen am 08.12.2020

Das Karlsruher Institut für Technologie (KIT) hat gemeinsam mit der Fraunhofer-Gesellschaft Thesen zur digitalen Souveränität Europas aufgestellt und dabei eine Differenzierung des Begriffs vorgenommen[3]. Es werden vier Dimensionen von digitaler Souveränität unterschieden:

- **Infrastruktursouveränität:** die Fähigkeit, technische Infrastrukturen vertrauenswürdig herzustellen oder ihre Vertrauenswürdigkeit zu prüfen und sie so zu betreiben, dass darauf angebotene Dienste vertrauenswürdig sein können.

- **Datensouveränität:** die Fähigkeit, informiert und selbstbestimmt zu entscheiden, wie und von wem Informationen über die eigene Person oder Institution, eigene Handlungen oder Produkte erhoben, verarbeitet und weitergegeben werden.

- **Entscheidungssouveränität:** die Möglichkeit, Ursprünge und Begründungen für Entscheidungen und Handlungsempfehlungen autonomer Systeme und Assistenten nachzuvollziehen und diese gegebenenfalls durch menschliches Eingreifen zu beeinflussen.

- **Plattformsouveränität:** Entsteht, wenn die Marktmacht großer Akteure in einer Plattformökonomie durch Regulierung und bewusste Kundenentscheidungen auf ein Maß beschränkt wird, das einen fairen Wettbewerb ermöglicht.

Wird auf Grundlage dieser Souveränitätsdimensionen über europäische Kompetenzen und gemeinschaftliche Güter gesprochen, so wird deutlich: Die EU-Mitgliedstaaten können in jedem einzelnen dieser vier Bereiche nur gemeinsam erfolgreich sein. Deutlich wird dies auch am Beispiel der Finanzwirtschaft.

3.2 Bedeutung für den Finanzsektor

Die digitale Souveränität Europas ist von erheblicher Bedeutung für die Innovationsfähigkeit europäischer Unternehmen und Organisationen. Dabei sind Anbieter- und Anwenderseite gleichermaßen zu berücksichtigen, da Anwender von IT-Dienstleistungen und Nutzer erfolgskritischer digitaler Technologien darauf angewiesen sind, dass es einen hinreichenden Wettbewerb auf der Anbieterseite gibt. Dies spüren auch Banken als Anwender einer Vielzahl von IT-Dienstleistungen seit Jahren. Der Aufbau einer konkurrenzfähigen europäischen IT-Anbieterlandschaft, prominent im Bereich Cloud, und eine aktive Förderung von europäischen IT-Kooperationsprojekten, wie zum Beispiel die GAIA-X-Initiative der Bundesregierung zur Schaffung einer offenen Dateninfrastruktur, sind von großer Bedeutung. Diese Initiativen zahlen auf die Dimension der **Infrastruktursouveränität** ein.

[3] https://www.fzi.de/fileadmin/user_upload/PDF/2017-10-30_KA-Thesen-Digitale-Souveraenitaet-Europas_Web.pdf, abgerufen am 08.12.2020

Damit in Verbindung stehen der Ausbau sicherer technologischer Infrastrukturen (z. B. 5G) und ein digitaler Euro. Zwar verfügt Europa mit dem auf dem SEPA-Standard aufsetzenden Zahlungsverkehr über eine souveräne und leistungsfähige Zahlungsinfrastruktur, diese wird jedoch durch Initiativen wie die Facebook-Gründung „Libra" (mittlerweile umbenannt zu „Diem") bedroht. Um einen programmierbaren Euro einzuführen und damit die Bedürfnisse der Industrie im Internet of Things (IoT) zu befriedigen, ist wiederum ein leistungsfähiges Telekommunikationsnetz unabdingbar. Echte digitale Infrastruktursouveränität kann obendrein nur durch starke europäische Kompetenz im Bereich Cybersicherheit erreicht werden, da dieser die sicherheitspolitischen Fragen der Zukunft dominieren wird.

Kern der Wertschöpfung in der digitalen Wirtschaft sowie strategischer Produktions- und Wettbewerbsfaktor sind Daten. Die Finanzwirtschaft unterstützt den Grundsatz der **Datensouveränität** mit der europaweiten Öffnung der Schnittstellen im Zahlungsverkehr seit Inkrafttreten der zweiten EU-Zahlungsdiensterichtlinie, kurz PSD2. Allerdings ist diese Öffnung heute einseitig und auf die Finanzwirtschaft begrenzt. Eine Schnittstellenöffnung ist nun für alle Branchen wie z.B. große Technologieunternehmen durchzusetzen, denn die Förderung des branchenübergreifenden Datenaustausches ist elementar für die europäische Datensouveränität. Diese schließt die freie Entscheidung der Kunden über Speicherung, Verarbeitung, Zugriff und Nutzung ihrer Daten zu jeder Zeit ein. Banken würde dies u.a. ermöglichen, Kundenbedürfnisse besser zu befriedigen und ihr Risikomanagement zu modernisieren und damit deutlich zu verbessern.

Die **Entscheidungssouveränität** im Digitalen hängt immer stärker von Kompetenzen auf dem Feld der künstlichen Intelligenz ab. Ganze Geschäftsmodelle und sogar staatliches Handeln basieren mehr und mehr auf der Auswertung riesiger Datenmengen durch komplizierte Algorithmen. Bereits in der COVID-19 Pandemie hat sich gezeigt, dass Entscheidungen basierend auf dem Einsatz fortgeschrittener KI-Systeme große Vorteile in der Pandemiebekämpfung bedeuten können.[4] Insbesondere die USA und China nehmen die Führungsrolle in Forschung und Entwicklung zu künstlicher Intelligenz ein. Fehlende europäische Kompetenzen auf diesem Gebiet können verheerende Folgen für die Souveränität Europas nach sich ziehen, da Technologien blindlings ohne echte Prüfungsmöglichkeiten eingekauft werden müssen. Bereits heute ist eine vollständige Rückverfolgung jeder Entscheidung beim Einsatz von fortgeschrittenen KI-Methoden, wie zum Beispiel von neuronalen Netzen, unter Umständen nicht mehr in allen Fällen möglich ist. Die Möglichkeit, Ursprünge und Begründungen für Entscheidungen und Handlungsempfehlungen autonomer Systeme nachzuvollziehen und gegebenenfalls beeinflussen zu können, ist wichtig für den Einzelnen ebenso wie für Unternehmen und Industrien. Hier muss mit Augenmaß gehandelt werden, um eine Entscheidungssouveränität gegenüber großen US-amerikanischen und chinesischen Technologieunternehmen durchzusetzen und gleichzeitig überbordende Regulierung für europäische Anbieter wie Banken zu vermeiden.

[4] https://thediplomat.com/2020/12/covid-19-underscores-the-benefits-of-south-koreas-artificial-intelligence-push/, abgerufen am 10.03.2021

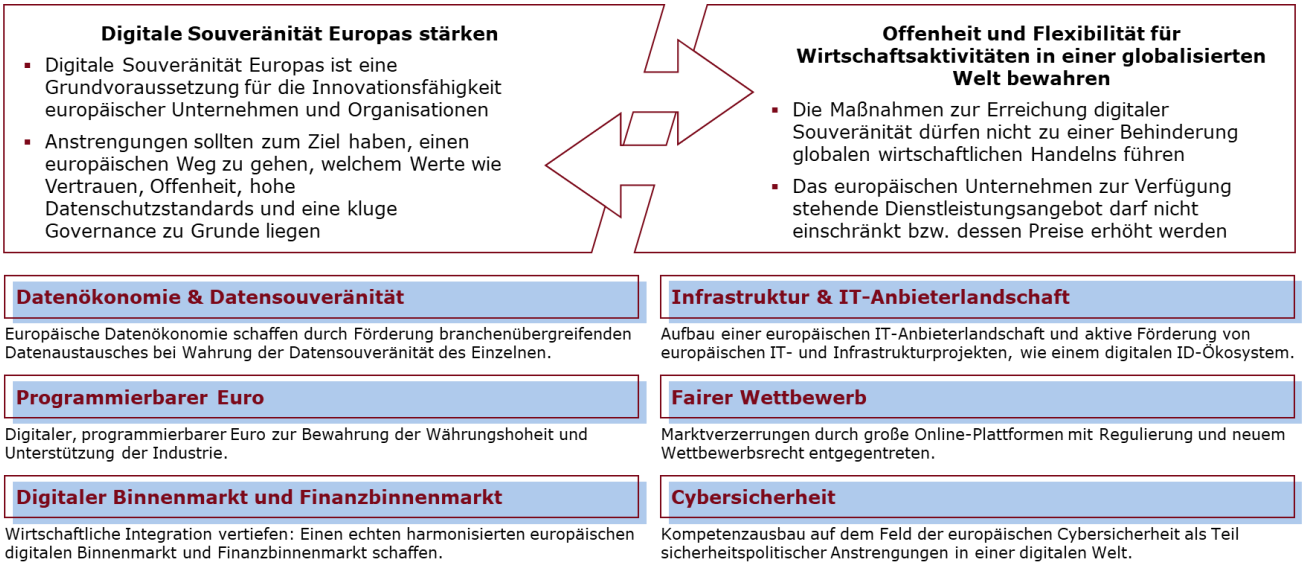

Abbildung 1

Im Sinne der **Plattformsouveränität** muss Marktverzerrungen, die aus der Gatekeeper-Funktion der großen Online-Plattformen resultieren, entgegengetreten werden: mit einer moderneren Regulierung digitaler Dienstleistungen und einem neuen Wettbewerbsrecht. Banken sind hier in besonderer Weise betroffen, da sie in einigen Geschäftsbereichen bereits in Konkurrenz zu großen Online-Plattformen stehen, zugleich aber auf Kooperationen mit diesen angewiesen sind, wie zum Beispiel beim Ausbau von Cloudlösungen in der Bank-IT. Insbesondere bei der Akquise von Neukunden sind Banken zunehmend von Plattformen abhängig; die Customer Journey beginnt meist bei Anbietern wie Google. Die Banken haben hier das Nachsehen, weil sie sukzessive die Kundenschnittstellen verlieren. Ein digitales europäisches Identitätsnetzwerk als Public-Private-Partnership zwischen allen Branchen und Regierungen könnte für den Bereich „Identifizierung" einen Gegenpol zu den Lösungen großer Plattformen bilden. Allerdings ist auch bei Bestandskunden eine enorme Abhängigkeit und der Verlust von Kundenschnittstellen zu beobachten, wie die Beispiele Apple Pay, Samsung Pay, Google Pay zeigen.

Digitale Souveränität sollte grundsätzlich nicht dadurch erreicht werden, dass bereits Bestehendes aus anderen Ländern kopiert wird, sondern durch eigene, in die Zukunft gerichtete Akzente, die auf einem europäischen Weg aufbauen. Dieser europäische Weg sollte geprägt sein von Werten und Standards wie Vertrauen, Offenheit, hohes Datenschutzniveau und kluger Governance. Viel Zeit aber haben wir nicht: Digitalisierung unterliegt keinem linearen Innovationsverlauf, sie ist exponentiell, und rasches Handeln sollte oberstes Gebot sein.

Im Folgenden stellen wir die spezifischen politischen Forderungen der privaten Banken vor, die mit der Absicht formuliert wurden, Europa auf dem Weg in die digitale Souveränität nach vorne zu bringen.

4 Politische Forderungen zur Stärkung der digitalen Souveränität Europas

4.1 Faire Bedingungen im digitalen Wettbewerb schaffen

- Die zunehmende Konzentration wirtschaftlicher Macht bei großen Online-Plattformen, die die Funktion von Gatekeepern der digitalen Wirtschaft einnehmen, sorgt für eine Verzerrung des europäischen digitalen Binnenmarktes und des globalen Wettbewerbs. Online-Plattformen können ihre Größenvorteile, Netzwerkeffekte und Datenbestände nutzen, um ihre Dienstleistungen ständig zu verbessern und in immer weitere Geschäftsfelder vorzudringen. Zugleich resultiert aus dem „Winner takes it all"-Effekt das Problem, dass bestehende oder potenzielle Konkurrenten und Neueinsteiger in vielen Fällen keine Möglichkeit haben, den Wettbewerbsvorsprung des Gatekeepers einzuholen.

- In einigen Geschäftsbereichen konkurrieren Banken bereits mit großen Online-Plattformen, in anderen sind sie auf Kooperationen mit ihnen angewiesen. Da Banken durch die Gatekeeper-Rolle großer Online-Plattformen in Gefahr geraten könnten, ihren direkten Kundenzugang an diese Plattformen zu verlieren, entscheiden sie sich teils selbst dazu, plattformbasierte Geschäftsmodelle zu adaptieren. Eine Differenzierung zwischen Gatekeeper-Plattformen und jungen, innovativen Plattformmodellen ist daher wichtig. Gerade Banken muss es erleichtert werden, Technologieentwicklungen sowie neue Geschäftsmodelle fernab des klassischen Bankgeschäfts in anderen Konzernbereichen zu betreiben, um einen langfristig wettbewerbsfähigen europäischen Finanzsektor zu erhalten.

- Einige Geschäftspraktiken großer Online-Plattformen sehen wir als besonders problematisch an, darunter fällt insbesondere der Ansatz „Take it or leave it", der darauf hinausläuft, dass Gatekeeper Verhandlungen oder Kompromisse in ihren Geschäftsbeziehungen oftmals gänzlich ausschließen. Wichtig ist in diesem Zusammenhang, dass große Gatekeeper-Plattformen nicht die Möglichkeit haben sollten, den Zugang zu technischen Infrastrukturen ihrer Plattformen einzuschränken, zum Beispiel durch die Limitierung des Zugangs zur NFC-Schnittstelle für Drittanwendungen im Finanzdienstleistungsbereich. Große Gatekeeper-Plattformen sollten obendrein zu mehr Datentransparenz und zum Teilen von Daten mit ihren Kunden (d. h. Unternehmen/Banken) verpflichtet werden.

- Wir unterstützen das Ziel, faire und wettbewerbsfähige Märkte zu erhalten. Denn Wettbewerb fördert Innovationen und kommt den Verbrauchern zugute. Wettbewerb steigert die Innovationsfreude der Unternehmen. Funktionierender Wettbewerb beugt gleichzeitig der Entstehung oder Verfestigung von zu starker gesellschaftlicher und politischer Machtstellung vor. Von einem wettbewerblich organisierten Markt profitieren insbesondere die Verbraucher,

weil sie aus einer breiten Angebotspalette diejenigen Güter und Leistungen auswählen können, die am ehesten ihren Vorstellungen hinsichtlich Qualität und Preis entsprechen.

- Der kürzlich von der EU-Kommission vorgelegte Vorschlag zum Digital Markets Act ist in diesem Zusammenhang ein Schritt in die richtige Richtung, da er die negativen Folgen adressiert, die sich aus Verhaltensweisen sehr großer Online-Plattformen (sog. Gatekeepern) – also Suchmaschinen, sozialen Netzwerken oder Online-Marktplätzen – ergeben. Der Vorschlag zielt darauf ab, Lücken in der Regulierung von Gatekeepern zu schließen und Durchsetzungsmaßnahmen zum Erhalt wettbewerbsfähiger Märkte zu ermöglichen. Die privaten Banken begrüßen die klare Begrenzung des Anwendungsbereichs dieser Regeln auf sehr große Online-Plattformen mit fest definierten quantitativen Schwellenwerten sowie die vorgesehenen klaren Ge- und Verbote. Die Regelungen des Digital Markets Act müssen nun auch schnellstens im europäischen Wettbewerb umgesetzt werden.

- In Deutschland hat der Gesetzgeber zu Jahresbeginn mit der 10. GWB-Novelle bedeutsame Änderungen des nationalen Wettbewerbsrechts auf den Weg gebracht, die sachgerecht auf die Zunahme der Bedeutung von Digital- und Plattformunternehmen reagieren. Dies sind insbesondere die Aufnahme der Intermediationsmacht als Kriterium zur Ermittlung einer marktbeherrschenden Stellung, die Neuregelung des Rechts auf Zugang zu essentiellen Infrastrukturen, Verhaltenspflichten für „Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb" sowie die kartellrechtliche Bewertung von Kooperationen durch das Kartellamt auf Antrag. Wir begrüßen diese Änderungen.

- Ein einheitlicher digitaler EU-Binnenmarkt ist Grundlage für eine wettbewerbsfähige und dynamische Marktentwicklung digitaler Dienstleistungen innerhalb der EU. Die existierende rechtliche Fragmentierung des digitalen EU-Binnenmarkts sollte gemindert werden, um Innovationschancen zu verbessern und den Binnenmarkt für digitale Dienste zu vertiefen.

  - Banken sehen sich in vielen Bereichen einer Fragmentierung von Regulierung, Aufsicht und Zuständigkeiten verschiedener Behörden im EU-Binnenmarkt gegenüber. Analog der Forderung der Banken nach einer Kapitalmarktunion in der EU ist ein digitaler Binnenmarkt für die sich immer mehr ins Digitale verlagernden Dienstleistungen der Banken von hoher Relevanz.

  - In den EU-Behörden muss hinsichtlich des Bereiches „Digital Services" ein wesentlich tieferer Kompetenzaufbau erfolgen und vor allem technisches Know-how akquiriert werden.

4.2 Cloud Banking in Europa fördern

- In der IT vieler Banken findet seit einigen Jahren ein technologischer Paradigmenwechsel statt. Angesichts des immer schnelleren Wandels von Branchen und Kundenbedürfnissen ist eine flexible und leistungsfähige IT-Infrastruktur lebenswichtig geworden. Getrieben von digitaler Konkurrenz und verändertem Kundenverhalten müssen bei verringerter Time-to-Market schrittweise Agilität, Kundenzentrierung und Kosteneffizienz erhöht werden.

  - Das Fundament dafür bildet die Cloud als technologische Grundlage für moderne Analytics-Lösungen, Anwendungen künstlicher Intelligenz, Big Data, Micro Services und API-Anbindungen. Meist ergibt sich im Zielbild der IT-Architektur der Bank ein hybrider Mix aus traditionellen IT-Systemen und Cloud-Anwendungen.

  - Die gezielte Migration der Bankinfrastruktur von lokalen Systemen in die Cloud ist dabei ein wichtiger Baustein, die Wettbewerbsfähigkeit der Bank der Zukunft zu sichern.

- Allerdings erschweren regulatorische Herausforderungen oftmals eine schnelle, effiziente und regelkonforme Umsetzung von Cloud-Projekten. Die Auslegung der vorhandenen Regulierung sowie deren Beaufsichtigung sind heute noch nicht ausreichend auf die rasant steigende Cloudnutzung in Banken abgestimmt. Gleichzeitig finden sich in neuen Regulierungsvorhaben wie zuletzt bei DORA (Digital Operational Resilience Act) auch Vorschläge, die die Cloud Journey der Banken behindern und nachteilige Effekte auf das Angebot an Cloud-Diensten oder deren Preise haben könnten. Um das zu ändern, sind aus unserer Sicht einige Anpassungen notwendig. Hier sind Regulatoren und Aufsichtsbehörden gefragt, sich als Unterstützer eines innovativen Finanzsektors aktiv an der Beseitigung praktischer Hürden für den breiteren Einsatz von Cloud-Technologien in Banken zu beteiligen.

- Wir sprechen uns für EU-weite, einheitliche Regeln und die Etablierung von Standards aus. Die Regulierung und Beaufsichtigung von Cloud-Auslagerungen sollten immer auf Grundlage eines risikobasierten Ansatzes erfolgen. Die Grundlage dafür ist bereits durch die existierende Regulierung[5] geschaffen. Die europäischen Banken haben zu diesen Forderungen zusammen mit der European Banking Federation (EBF) mehrere technische Positionspapiere[6] veröffentlicht, die einen edukativen Ansatz verfolgen und zum Diskurs anregen sollen.

  - Ein gemeinsames Verständnis der Risiken und verfügbaren Kontrollmechanismen für Cloud-Services ist unerlässlich. Die Bewertung der Risikodimension sollte anhand einheitlicher Kriterien, wie Grad der Verantwortungsübertragung und Bedeutung der ausgelagerten Daten und Funktionen, geschehen.

---

[5] https://www.eba.europa.eu/documents/10180/2761380/EBA+revised+Guidelines+on+outsourcing_DE.pdf/5546a705-bff2-43eb-b382-e5c7bed3a2bc, abgerufen am 10.03.2021

[6] https://www.ebf.eu/priorities/cybersecurity-innovation/cloudbanking/, abgerufen am 21.12.2020

- Die Anforderungen für das Reporting an Aufsichtsbehörden sowie an Exit-Strategien (z. B. Geschäftsfortführung bei Kündigung des Auslagerungsnehmers oder erheblichem Serviceausfall, etc.) müssen europaweit klar und einheitlich sein.

- Derzeit ist eine Konzentration auf einige wenige, sehr große globale Cloud-Infrastruktur-anbieter zu beobachten. Um daraus resultierende Abhängigkeiten zu minimieren, sollten industrieübergreifende Standards unterstützt werden, die eine grundsätzliche Übertragbarkeit von Daten zwischen Cloud-Anbietern sicherstellen. Mit diesem Ziel wurde 2020 industrie-übergreifend SWIPO[7] (Switching Cloud Providers and Porting Data) mit Unterstützung der Europäischen Kommission als Verbund verschiedener Stakeholder gegründet. Die Initiative hat einen Code of Conduct zur Verhinderung von Vendor Lock-in entwickelt. Daneben sollte die in der Diskussion stehende Beaufsichtigung von Cloud-Anbietern keine nachteiligen Effekte auf die Nutzung von Cloud-Services durch Banken haben.

- Die von der Bundesregierung initiierte Initiative GAIA-X könnte ein weiteres Mittel sein, den Cloudmarkt transparenter zu gestalten und dadurch den Kreis der Cloud-Anbieter zu vergrößern. Wir begrüßen die Initiative und bringen uns aktiv in der Domäne Finanzwesen sowie in das Förderprojekt „Financial Big Data Cluster" ein. GAIA-X wird allerdings die etablierten Cloud-Anbieter nicht ersetzen, sondern als eine zusätzliche Alternative im Markt dienen.

  - Die europäische Finanz- und Versicherungscommunity in GAIA-X hat sich auf „Compliance by Design" als eine Kernforderung verständigt. Dies bedeutet, dass alle mit dem GAIA-X-Label versehenen Dienste bereits bei Veröffentlichung, also ex-ante, konform mit der Finanzmarktregulierung sein müssen.

  - Die breite Unterstützung und Einbindung von relevanten Ressorts und Aufsichtsbehörden muss bereits von der Entwicklungsphase an in GAIA-X erfolgen. Damit könnte GAIA-X schließlich auch dazu beitragen, dass die Cloud-Regulierung den Anforderungen der Finanzbranche besser Rechnung trägt.

4.3 Förderung der Datenökonomie durch Schaffung eines branchenübergreifenden Datenrahmens

- Daten sind Kern aller Wertschöpfungsprozesse in der digitalen Wirtschaft und damit strategischer Produktions- und Wettbewerbsfaktor; sie tragen maßgeblich zum wirtschaftlichen Erfolg von Unternehmen und Volkswirtschaften bei.

[7] https://swipo.eu/, abgerufen am 21.12.2020

- Eine europäische Datenökonomie eröffnet im internationalen Standortwettbewerb die Chance, durch datengetriebene Innovationen die Wettbewerbsfähigkeit des Kontinents entscheidend zu stärken.

- Der Zugang zu Daten und ihre Wiederverwendungsmöglichkeit sind dabei entscheidende Erfolgsfaktoren und tragen zur digitalen Souveränität Europas bei.

- Die Rahmenbedingungen einer Datenökonomie müssen allen Marktteilnehmern gleiche Chancen ermöglichen, das Teilen von Daten unter fairen Bedingungen fördern und zugleich den Schutz von persönlichen Daten und Geschäftsgeheimnissen bewahren.

- Der derzeitige Rechtsrahmen schafft Asymmetrien, bei denen einige Unternehmen – insbesondere etablierte Technologiekonzerne – als Daten-Gatekeeper agieren, wohingegen Banken den Zugriff zu ihren Kundendaten einseitig ermöglichen müssen. Es fehlt die Gegenseitigkeit, was sich negativ auf die digitale Souveränität Europas auswirkt.

- Angesichts der steigenden Marktdurchdringung und Diversifizierung von außereuropäischen Technologiekonzernen bzw. Plattformunternehmen könnten sektorspezifische Ansätze die Ungleichgewichte weiter erhöhen. Ein branchenübergreifender Datenaustauschrahmen könnte dem entgegenwirken.

- Aus Sicht des Bankenverbandes bedarf es eines europäischen Rechtsrahmens, der einen Datenaustausch über verschiedene Unternehmen und Industrien hinweg ermöglicht:

  - Hinsichtlich **personenbezogener Daten** sollten Unternehmen aller Branchen dazu verpflichtet werden, die von einer Person bereitgestellten Daten in Echtzeit via Standard-Mechanismen dann zu teilen, wenn der Betroffene dies wünscht. Hiermit könnte bestehendes Recht zur Datenportabilität nach DSGVO operationalisiert werden und zu neuen Services und Kundenmehrwerten führen.

  - Zudem müssen Datenkooperationen zum Austausch **nicht-personenbezogener** Daten erleichtert werden, unter anderem dadurch, dass mehr Rechtssicherheit (z. B. hinsichtlich der Anonymisierung) geschaffen wird. Solche Kooperationen, zum Beispiel in Form des Datenpooling, sind ein wesentlicher Erfolgsfaktor, um aus der Analyse verschiedenster Daten neue Erkenntnisse zu gewinnen und die Potenziale von künstlicher Intelligenz und maschinellem Lernen für die Forschung und die Wirtschaft in Europa zu erschließen.

  - Ferner sollte der Zugang zu **Daten des öffentlichen Sektors** konsequent vorangetrieben werden. Hierbei ist neben der Etablierung von standardisierten elektronischen Zugangsmöglichkeiten die Konsolidierung der Zugangspunkte im öffentlichen Sektor wünschenswert, um Transaktionskosten zu reduzieren und die Daten einer möglichst breiten Nutzung zuzuführen.

- Die von der EU-Kommission im Rahmen der **Data-Governance-Verordnung** vorgeschlagenen Instrumente zur Förderung der Datenverfügbarkeit und -nutzung, insbesondere durch Erhöhung des Vertrauens in Datenintermediäre über einen gesetzlichen Anmelde- und Aufsichtsrahmen, können zusätzliche Impulse geben. Sie allein dürften aber nicht ausreichen, um eine europäische Datenökonomie Wirklichkeit werden zu lassen.

4.4 Kompetenzausbau Cybersicherheit

- In den letzten Jahren hat sich die Gefahr von Cybervorfällen verschärft. Dies liegt insbesondere an den technologischen Entwicklungen und der stärkeren Vernetzung der Unternehmen, aber auch an der zunehmenden Professionalisierung der Cyberkriminellen und Angreifer. Nicht umsonst werden Cyberangriffe heute als das größte operationelle Risiko im Finanzsektor angesehen. Dementsprechend ist es unbedingt erforderlich, den eingeschlagenen Weg zur stetigen Verbesserung der Cyber-Widerstandsfähigkeit Europas konsequent weiter zu verfolgen.

- Mit der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (Digital Operational Resilience Act - DORA) hat die Europäische Kommission nun einen Vorschlag für die Harmonisierung der IT-(Sicherheits-)Regulierung im Finanzsektor vorgelegt. Diese Koordinierung bzw. Harmonisierung der regulatorischen Anforderungen ist unbedingt notwendig, um Synergieeffekte und Effektivitätssteigerungen in den Sicherheitsarchitekturen der Banken zu schaffen und die Cyber-Resilienz in Europa zu stärken. Außerdem müssen hierdurch unverhältnismäßiger Aufwand, Doppelbelastungen und Unsicherheiten angesichts heute noch divergierender Anforderungen wegfallen. Die dadurch frei gesetzten Ressourcen stärken wiederum die Banken beim Ausbau ihrer eigenen Cyber-Abwehrmaßnahmen und Reaktionsmöglichkeiten.

- Für die anstehenden Aufgaben sind europäische IT-Expertinnen und Experten gefragter als jemals zuvor. Ihre Aus- und Fortbildung bzw. Verfügbarkeit auf dem Markt ist heutzutage eine der wesentlichen Herausforderungen. Studien belegen[8] aktuell ein Defizit von knapp 170.000 Expertinnen und Experten allein für Europa – Schätzungen liegen bei 350.000 für das Jahr 2022. Das wirkt sich negativ auf das Sicherheitsniveau der Unternehmen aus. Doch bei der – sich aktuell deutlich beschleunigenden – Digitalisierung darf die IT- und Informationssicherheit nicht zu kurz kommen. Daher ist es unerlässlich, in die Ausbildung von IT-Fachkräften zu investieren.

- Darüber hinaus ist die unternehmens- und sektorübergreifende Vernetzung der Cybersicherheitsverantwortlichen essenziell. Die Verflechtung der staatlichen und privatwirtschaftlichen

[8] Cybersecurity Workforce Study von 2020 und 2018; Cyber-Sicherheits-Studie von Trend Micro 2019

Sicherheitsereignis- und Reaktionsteams ist eine wesentliche Voraussetzung, um mögliche Großereignisse bewältigen zu können. Ereignisfeststellung, -bewertung und gegebenenfalls die Krisenreaktion sind in der Cybersicherheit eine Gemeinschaftsaufgabe und müssen auch als solche bewältigt werden.

- Ergänzend sei schon jetzt auf die zukünftigen Auswirkungen von Quantencomputern auf die Sicherheit der derzeit im Einsatz befindlichen kryptografischen Sicherheitsverfahren hinzuweisen. Um sich zukünftig vor Cyber-Angriffen mithilfe von Quantencomputern schützen zu können, müssen Unternehmen, Sicherheitsindustrie und relevante nationale und supranationale Behörden an einem Strang ziehen und geeignete Lösungskonzepte konzipieren und rechtzeitig umsetzen. Nur dann können die Vorteile und Potenziale der neuen Technologie sinnvoll genutzt, die Sicherheitsrisiken erkannt und diesen effizient entgegengewirkt werden.

- Die europäische Marschrichtung wird zweifellos auch einen Einfluss darauf haben, wie Fragen der Cybersicherheit auf globaler Ebene adressiert werden. Am Ende bedarf es koordinierter Maßnahmen und gemeinsamer Bemühungen von Politik, Aufsichtsbehörden, Zentralbanken und Finanzindustrie. Dabei sollten auch kollektive Maßnahmen von Regierungen zur Abschreckung böswilliger Cyber-Aktivitäten, die sich gegen Finanzinstitute richten, geprüft werden, wie zum Beispiel internationale Normen und diplomatische Prozesse zur Erhöhung der Cyberstabilität.

4.5 Einführung eines programmierbaren Euro

- Distributed Ledger Technologie (DLT) und Smart Contracts werden die Wirtschaftsabläufe in vielen Bereichen aller Industrien grundlegend verändern. Sie werden ihr Potenzial aber nur dann voll entfalten können, wenn auch Bezahlvorgänge in Smart Contracts eingebunden sind. Effizient und ohne Systembruch ist dies nur mit programmierbarem Geld auf einer DLT möglich.

- Die Verfügbarkeit einer programmierbaren Form des Euro wird deshalb über die internationale Wettbewerbsfähigkeit der Unternehmen in Deutschland und Europa im Konkurrenzkampf Europas mit Asien und Nordamerika mitentscheiden. Die Diskussion um Libra/Diem hat daher einen wichtigen Anstoß zur Diskussion um die Gestaltung der globalen Geld- und Währungsordnung für das digitale Zeitalter gegeben.

- Jedoch müssen neue auf DLT basierende Geldformen so in die Geld- und Währungsordnung integriert werden, dass deren **Stabilität und Widerstandsfähigkeit nicht gefährdet werden.**

- Das Eigenschaften des zweistufigen Bankensystems sollten sich auch in den neuen Geldformen widerspiegeln. So sollte die EZB mit einem digitalen Euro die grundlegende

Funktion des Zentralbankgeldes aufrechterhalten, die Stabilität anderer Geldformen, wie etwa Giralgeld, gewährleisten und dadurch die Entwicklung und Vielfalt der Geldformen ermöglichen.

- Die Privaten Banken sehen sich vor der Aufgabe Giralgeld zu einer programmierbaren Geldform, dem Giralgeldtoken, weiterzuentwickeln.
- Die **privaten Banken schlagen ein dreistufiges Vorgehen** vor:
  - Eine **Anpassung des bestehenden Zahlungsverkehrssystems** in Europa an die Herausforderungen der Digitalisierung, insbesondere eine Verbesserung und Optimierung von **TIPS und EPI**.
  - Bündelung der Kräfte der deutschen und europäischen Kreditwirtschaft zur Gestaltung und Emission eines **Tokens auf Basis des Giralgeldes** (Giralgeldtoken).
    Eine gemeinschaftliche und auf privatrechtlichen Vereinbarungen basierende Lösung ist erforderlich, weil nur so die Interoperabilität und Konvertibilität, der von einzelnen Banken geschaffenen Token gewährleistet werden kann.
    Eine Unterstützung durch eine europäische Regulierung zur Schaffung von Standards – in Analogie zu SEPA/PSDII – sollte diesen Prozess befördern.
  - Vorantreiben der Bemühungen um die **Bereitstellung eines digitalen Zentralbankgeldes (CBDC) für die breite Öffentlichkeit**. Dabei ist mit größter Sorgfalt vorzugehen, damit die Funktionalität des bestehenden Finanzsystems einschließlich der Banken nicht beschädigt wird.
    Es wird insbesondere darauf ankommen, dass der Zugang zu CBDC nur über das Bankensystem erfolgen kann. Dies ist eine der Voraussetzungen, um die Risiken von CBDC – namentlich Disintermediation und Bank Run – zu minimieren.
  - In jedem Fall sind alle Bemühungen mit Blick auf „Time-to-Market" zu intensivieren, um nicht durch reaktives Verhalten den Anschluss in der Diskussion zu verlieren und das zukünftige Zielbild nicht mehr mitgestalten zu können.
- Selbstverständlich muss gewährleistet werden, dass die weltweit in der Entstehung begriffenen Geldformen auf DLT-Basis international konvertierbar sind. Dies setzt aufeinander abgestimmte internationale Regulierungsmaßnahmen voraus. Die Erfahrung aus der Finanzkrise hat allerdings gezeigt, dass dies sehr zeitaufwendig ist und der internationale Konsens sehr schnell brüchig werden kann.

4.6 Schaffung eines digitalen ID-Ökosystems

- Für den digitalen Wirtschaftsverkehr benötigen wir einfach nutzbare, sichere sowie rechtlich anerkannte und wiederverwendbare digitale Identitäten. Derzeit sind diese nicht vorhanden.

- Um digitalen Identitäten zum Durchbruch zu verhelfen und bestehende Barrieren zu überwinden (z. B. mangelnde Verbreitung), setzen wir uns für die Schaffung eines nationalen und in zweiter Stufe europäischen ID-Ökosystems ein.

- Ein digitales ID-Ökosystem verspricht den reibungslosen Austausch von Identitätsdaten und -merkmalen natürlicher und juristischer Personen und womöglich auch von Dingen („Internet of Things") – und dies über unterschiedliche Branchen und Anwendungsfälle in der Privatwirtschaft und der öffentlichen Hand.

- Voraussetzung hierfür ist, dass der Dschungel an unterschiedlichen gesetzlichen Anforderungen und Aufsichtspraktiken an die Identifizierung beseitigt wird, innerhalb der EU und mit Blick auf die verschiedenen Sektoren (Banken und andere geldwäscherechtlich Verpflichtete, Vertrauensdienste, Telekommunikationsanbieter, öffentlicher Sektor). Anderenfalls droht standortabhängig eine Benachteiligung einzelner europäischer Anbieter gegenüber ihren EU-Wettbewerbern, wie dies derzeit zum Beispiel bei deutschen Vertrauensdiensten zu beobachten ist.

- Banken sind gesetzlich zur Kundenidentifizierung verpflichtet und haben daher großes Interesse, zuverlässige digitale Identitäten für ihre Kundenprozesse zu nutzen. Gleichzeitig können sie hochwertige und verlässliche Identitätsdaten ihrer Kunden im weiteren Sinne (z. B. Ausweisdaten, Einkommensnachweise, Kontodaten) in ein Ökosystem einbringen.

- Die heute in Deutschland mangelnde Verfügbarkeit an breit nutzbaren, qualifizierten digitalen Identitäten kann – zumindest übergangsweise – durch eine bessere Wiederverwertbarkeit von verifizierten Kundenidentitäten, die zum Beispiel durch Banken im Rahmen des Know-Your-Customer-Prozesses erhoben wurden, ausgeglichen werden.

- Im Sinne der digitalen Souveränität des Einzelnen ist es wichtig, allen Bürgern die Möglichkeit zu geben, selbstbestimmt darüber entscheiden zu können, wie ihre Daten genutzt werden. Dies gilt zuallererst für Daten, die unmittelbar die eigene Identität betreffen. Verbraucher sollten jederzeit Transparenz darüber und es selbst in der Hand haben, wem sie zu welchen Zwecken ihre Identitätsdaten zur Verfügung stellen.

- Einen Lösungsansatz hierfür bieten digitale selbstbestimmte Identitäten bzw. Self-Sovereign Identities (kurz „SSI"), bei denen Bürger ihre eigenen Identitätsdaten selbst verwalten und bedarfsweise für die Nutzung durch einen Dritten, zum Beispiel bei Begründung einer Vertragsbeziehung oder Inanspruchnahme einer Dienstleistung, freigeben. Nur die Nutzer

selbst kennen alle ihre Identitätsdaten und entscheiden selbstbestimmt, mit wem diese Daten geteilt werden.

- Wir begrüßen daher die jüngste Initiative der Bundesregierung für ein europäisches Ökosystem digitaler Identitäten auf Grundlage eines SSI-Ansatzes und teilen die Einschätzung, dass ein solches Ökosystem nur im Rahmen einer engen Zusammenarbeit zwischen Privatwirtschaft und dem öffentlichen Sektor (Institutionen und Behörden) zu erreichen ist.

- Der Bankenverband hat mit seinen Mitgliedern (Banken und FinTechs) Vorschläge erarbeitet, wie ein solches Ökosystem Realität werden kann und in einem separaten Positionspapier „Digitale Identitäten – Schritte auf dem Weg zu einem ID-Ökosystem" veröffentlicht.