DIE AUFHEBUNG DER LOKALISIERUNGSVERPFLICHTUNGEN FÜR DATEN

ZUSAMMENFASSUNG

Die Kommission beabsichtigt, den Grundsatz des freien Datenverkehrs in Europa zu schaffen. **Eine der wichtigsten Auswirkungen bei der Einführung dieses Grundsatzes wäre die Einschränkung der nationalen Verpflichtungen in Bezug auf die Datenlokalisierung, die dann nur mehr in Ausnahmefällen zum Tragen kommen würde**[1]. Mit der Einführung dieses Grundsatzes soll das wirtschaftliche Potential eines einheitlichen Datenmarktes auf europäischer Ebene freigesetzt werden, indem man gegen die geographische Fragmentierung dieses Marktes vorgeht.

Der Rat teilt die von der Kommission angepeilten Ziele, ist jedoch der Ansicht, dass **die Verankerung eines solchen Grundsatzes im gegenwärtigen Stadium nicht opportun ist**. Die größten Barrieren für das Wachstum einer innovativen Datenwirtschaft sind nämlich **weniger auf die nationalen Grenzen zurückzuführen, sondern eher auf die Lock-in und Zurückhaltestrategien von Daten zwischen den Akteuren der Wirtschaft**. Der Grundsatz des freien Datenverkehrs müsste sich daher mehr auf den Datenverkehr zwischen Plattformen als zwischen Staatsgebieten beziehen.

Außerdem entsteht die **geographische Fragmentierung des Datenmarktes** – und insbesondere des *Cloud computing*-Marktes – **auf europäischer Ebene nur begrenzt durch gesetzliche Lokalisierungsvorschriften**. Letztere betreffen nur einen sehr geringen Teil der in Europa produzierten Daten. In Frankreich gibt es beispielsweise lediglich fünf Texte, in denen Lokalisierungsvorschriften enthalten sind. **Die Forderung einer Datenlokalisierung ist in erster Linie auf Verbraucherpräferenzen zurückzuführen**, was einen großen Mangel an Vertrauen in die *Cloud computing*-Wirtschaft zum Ausdruck bringt. Außerdem stellen die **mangelnde Vereinheitlichung der anderen Binnenmärkte (Waren, Dienstleistungen, Kapital...) und die mangelnde Abstimmung in Bezug auf steuerliche Regelungen heute eine größeres Hindernis für die Entwicklung** von europäischen Akteuren des *Cloud computing* dar.

Und schließlich kann der Grundsatz des freien Datenverkehrs die Fähigkeit der Staaten einschränken, Regulierungen in Bereichen durchzuführen, die mit der legitimen Ausübung ihrer Staatshoheit in Zusammenhang stehen. Buchhaltungs- und Finanzdaten müssen zum Beispiel lokalisiert werden, um steuerliche Kontrollen durchführen zu können. Auch wenn es sehr wohl Kooperationsmechanismen gibt, um den Datenzugang über Landesgrenzen hinweg zu erleichtern, könnte die Lokalisierung von Daten außerhalb der Staatsgrenzen trotzdem die Durchführung solcher Kontrollen erschweren und verlangsamen und sogar das Verschwinden von Dokumenten und Belegen begünstigen. Darüber hinaus scheint es abgesehen von diesen mit den aktuellen Lokalisierungsverpflichtungen verbundenen Risiken gefährlich, die Regulierungsfähigkeit der Staaten in Zukunft einzuschränken, wenn man die Unsicherheiten bedenkt, die potentielle Nutzungen belasten, und dies inmitten neuer Wirtschaftsmodelle.

Der Rat empfiehlt daher eher, die Lokalisierungsverpflichtungen aufeinander abzustimmen, als diese Verpflichtungen grundsätzlich aufzuheben, um die Komplexität der rechtlichen Bestimmungen innerhalb des europäischen Datenmarktes in Grenzen zu halten. **Diese Harmonisierung sollte gleichzeitig mit der Einführung von klaren Normen und Standards in Bezug auf die Sicherheit von und den Zugang zu gespeicherten Daten nach dem neuesten Stand der Technik vor sich gehen**. Dadurch wird es möglich sein, einen einheitlichen Datenraum zu schaffen, für den strenge Kriterien zum Schutz gelten, und man wird Dumping-Phänomene und Kontrollverluste bei Daten vermeiden können.

Die Europäische Kommission hat angekündigt, dass im Herbst 2018 eine Gesetzesinitiative in Bezug auf die Aufhebung der nationalen Verpflichtungen für Datenlokalisierung initiiert wird, was durch die Schaffung eines Grundsatzes des freien Datenverkehrs erreicht werden soll.

Viele Mitgliedstaaten haben tatsächlich Datenlokalisierungsverpflichtungen in verschiedenen Bereichen ihrer staatlichen Politik eingeführt. *Dies betrifft die nationale Sicherheit, die Effizienz der von den Steuerbehörden durchgeführten Kontrollen, die Erhaltung staatlicher Archive, die Vorschriften für Spiele im Internet. Mit diesen Verpflichtungen, die von Land zu Land verschieden sind, kann die Ausweitung der Auslagerung von Datenspeicherung und im weiteren Sinne auch des Cloud computing über Landesgrenzen hinweg eingebremst werden.* ***Das von der Europäischen Kommission verfolgte Ziel besteht daher darin, gegen die Fragmentierung des europäischen Datenmarktes anzukämpfen****. Die Vereinheitlichung der europäischen IT-Märkte soll insbesondere zur Entwicklung von europäischen Spitzenanbietern des Cloud computing führen.*

DIE AUFHEBUNG DER VERPFLICHTUNGEN FÜR DIE DATENLOKALISIERUNG KÖNNTE IHR ZIEL VERFEHLEN

Die Landesgrenzen stellen nicht die wichtigsten Barrieren für die Entwicklung einer europäischen Datenwirtschaft dar

Mit der Einführung eines Grundsatzes des freien Datenverkehrs sollen in erster Linie die Datenbewegungen zwischen Ländern erleichtert werden, wie dies bereits früher bei anderen Märkten durchgeführt werden konnte (Waren, Dienstleistungen, Kapital). Bei der Vereinheitlichung eines solchen Marktes stellt sich insbesondere die Frage der Schaffung eines europäischen *Cloud computing*-Marktes, und zwar sowohl, was die Nachfrage als auch was das Angebot betrifft. Angesichts des Vorsprungs, den die dominanten Akteure des Cloud-Marktes erreicht haben, scheint es notwendig, die Entstehung neuer innovativer Akteure zu fördern.

Es scheint jedoch, dass die wesentlichen Hindernisse für das Wachstum eines innovativen Datenmarktes weniger auf die Landesgrenzen infolge der Lokalisierungsbeschränkungen zurückzuführen sind, sondern eher auf die **Lock-in und Zurückhaltestrategien von Daten zwischen Akteuren der Wirtschaft.** Man sollte sich daher vorrangig auf Barrieren gegen den Datenverkehr zwischen Plattformen und weniger zwischen Ländern konzentrieren, insofern, als die digitale Wirtschaft besonders durch die Wirkung von « Datensilos » gekennzeichnet ist, die Innovationshindernisse darstellen können.

Die geographische Fragmentierung des Datenmarktes wird nur in geringem Ausmaß durch gesetzliche Lokalisierungsverpflichtungen verursacht

- **Innerhalb der EU-Mitgliedstaaten wurden nur wenige gesetzliche Lokalisierungsverpflichtungen erlassen**

Aufgrund der im Jahr 2016 beschlossenen Datenschutz-Grundverordnung (DSGVO) konnte ein bedeutender Fortschritt erreicht werden. Dadurch wurde ein einheitlicher Rahmen für den Schutz personenbezogener Daten in Europa geschaffen. Außerdem ist somit die Aufhebung der Lokalisierungsverpflichtungen für Daten innerhalb Europas infolge des Schutzes der personenbezogenen Daten gerechtfertigt.

Lokalisierungsverpflichtungen aus anderen Gründen als für den Schutz personenbezogener Daten betreffen nur **einen sehr geringfügigen Teil** der in Europa produzierten Daten. In Frankreich wurden beispielsweise lediglich fünf Texte für derartige Verpflichtungen erlassen. Diese Texte beziehen sich auf spezielle Arten von Daten und Situationen, manchmal im Umfeld der Datenschutz-Grundverordnung (DSGVO), oder auch außerhalb der europäischen Verträge, so dass sie von der Einführung eines Grundsatzes des freien Datenverkehrs nicht betroffen sind (Patientendaten, militärische Geheimdokumente). Außerdem ist eine gewisse Anzahl von Lokalisierungen auf eine **fehlerhafte Auslegung** dieser Verpflichtungen zurückzuführen. Viele Akteure in diesem Markt sind nämlich der Ansicht, dass die Speicherung und Bearbeitung von Daten innerhalb der Landesgrenzen verpflichtend oder empfohlen ist, was jedoch nicht der Fall ist[2].

- **Die Präferenzen von Verbrauchern sind für den Großteil der Lokalisierungen bestimmend**

Viele Unternehmen beschließen, ihre Daten nicht aus gesetzlichen Gründen in ihrem Land zu speichern, sondern, um sich nach den Präferenzen von Verbrauchern zu richten. Die Lokalisierung wird in der Tat von vielen als Garant einer größeren Sicherheit, besseren Geheimhaltung und Integrität der Daten betrachtet. 37,7 % der Nutzer des *Cloud computing* haben größeres Vertrauen in die Sicherheit ihrer Daten, wenn diese in ihrem Land gespeichert und bearbeitet werden[3]. **Wenn also Anbieter der Cloud ihre Infrastrukturen auf den verschiedenen europäischen Märkten ausbauen müssen, geht es nicht so sehr darum, sich an gesetzliche Verpflichtungen zu halten, sondern auf die Anforderungen ihrer Kunden zu reagieren**. Und diese Anforderungen zeigen aus verschiedenen Gründen ein größeres Misstrauen gegenüber dem *Cloud computing*, nämlich eine Unsicherheit bezüglich der Kontinuität und der Qualität dieser Leistungen, tatsächliche oder befürchtete Schwierigkeiten hinsichtlich einer effizienten Integration der Applikationen in das übrige IT-System, Schwierigkeiten, die mit der *Cloud* verbundenen Standards zu akzeptieren[4]... Diesem Misstrauen kann durch bessere Information und Schulung der Akteure der Wirtschaft im Hinblick auf die mit dem *Cloud computing* verbundenen Herausforderungen begegnet werden.

- **Die fehlende Harmonisierung der anderen Binnenmärkte hat stärkere Auswirkungen auf die Fragmentierung des Datenmarktes**

Die fehlende Harmonisierung der anderen Binnenmärkte (Waren, Dienstleistungen, Kapital...), aber auch im Hinblick auf Steuervorschriften, scheint zum jetzigen Zeitpunkt ein größeres Hindernis für die Entwicklung der europäischen Akteure des *Cloud computing* darzustellen als es die Lokalisierungsverpflichtungen sind. Die Unterschiede in den steuerlichen Vorschriften oder den Bestimmungen des Verbraucherrechts haben für IT-Anbieter große Auswirkungen auf die Fragmentierung des Marktes.

ES FEHLEN SOLIDE GARANTIEN HINSICHTLICH DER ZUGANGSBEDINGUNGEN FÜR STAATEN UND IN BEZUG AUF DIE SICHERHEIT

- **Der Zugang der Behörden zu Daten muss aufrecht erhalten werden**

Mit Hilfe der Lokalisierungsverpflichtungen soll in erster Linie sichergestellt werden, dass Staaten zu bestimmten Daten Zugang haben. Die Verpflichtungen hinsichtlich der Buchhaltungsdaten waren zum Beispiel darauf ausgerichtet, es den Steuerbehörden zu ermöglichen, ihre Kontrollfunktionen unter besten Bedingungen auszuüben, insbesondere, was gerichtliche Durchsuchungen betrifft. In Bezug auf Durchsuchungen und die Beschlagnahme von Daten im Rahmen von steuerlichen Ermittlungen existieren je nach Land unterschiedliche Regeln. Auch scheint es legitim, dass Staaten alles das, was ihre Staatsarchive und ihr nationales Kulturgut umfasst, innerhalb ihres Territoriums aufbewahren können. Wenn in diesem speziellen Fall auch die potentiellen Zugangsschwierigkeiten nicht so groß sein werden wie im Fall von Buchführungsdaten, die im Ausland gespeichert sind und die Gegenstand einer absichtlichen Verschleierungsstrategie sein können, so kann jedenfalls der Zugang zu Archiven für den Staat schwieriger sein, wenn sich diese im Ausland befinden – beispielsweise auch aus diplomatischen Gründen.

Die Zugangsbedingungen sind, vor allem was den Zugang für Gerichte betrifft, innerhalb der EU-Mitgliedstaaten noch wenig aufeinander abgestimmt. Vor der Sanktionierung des Grundsatzes des freien Datenverkehrs ist es daher notwendig, aufeinander abgestimmte europäische Zugangsbedingungen sowohl in rechtlicher Hinsicht als auch mit den entsprechenden technischen Kapazitäten einzurichten.

- **Hohe Sicherheitsstandards müssen gemeinsam festgelegt werden**

Mit Hilfe der Lokalisierungsverpflichtungen soll auch die Sicherheit der gespeicherten Daten aufrecht erhalten werden. Dieses Argument scheint hinfällig zu sein, denn ab nun hängt die Sicherheit der gespeicherten Dokumente weniger von ihrer physischen Lokalisierung ab, sondern von den Kapazitäten in Bezug auf die Verschlüsselung und die Cybersicherheit, die zum Datenschutz angewendet werden. Die Lokalisierung selbst scheint daher kein besseres Sicherheitsniveau zu garantieren. Den Lokalisierungsverpflichtungen entspricht jedoch trotz allem die Durchsetzung eines nationalen Rechts im Hinblick auf Sicherheitsstandards, insbesondere im Bereich der Informationstechnologie.

Es scheint daher notwendig, **vor der Sanktionierung des Grundsatzes des freien Datenverkehrs die IT-Sicherheitsstandards in den Ländern der Europäischen Union einander anzugleichen, damit die Aufhebung der Lokalisierungsverpflichtungen nicht zu einer Verschlechterung des Sicherheitsniveaus und zu « Dumpingeffekten » innerhalb der Union führt**. Dieses Standards dürfen sich nicht auf eine bloße gegenseitige Anerkennung der Gleichwertigkeit der Sicherheitsbedingungen zwischen europäischen Ländern beschränken. Diesbezüglich scheint das Modell der Regulierung für personenbezogene Daten durchaus zielführend: Die Lokalisierungsverpflichtungen werden aufgehoben, insoweit als eine weitgehende Angleichung der Sicherheits- und Schutzbedingungen für persönliche Daten durchgeführt wurde. Es geht darum, nach dem neuesten Stand der Technik vorzugehen und systematisch und obligatorisch alle Sicherheitslücken aufzuzeigen, um Verbesserungen des Sicherheitsniveaus für das gesamte europäische Ökosystem zu fördern.

DER RAHMEN FÜR DIE ANGLEICHUNG DER LOKALISIERUNGSBEDINGUNGEN MUSS FESTGELEGT WERDEN

- **Die tatsächlichen Auswirkungen auf die Fähigkeit der Staaten, regulierend einzugreifen**

Im Vorfeld müssen echte **Studien über die Auswirkungen auf die Staaten** durchgeführt werden, um die Gefahren zu beurteilen, denen die Staaten aufgrund der Aufhebung der Lokalisationsverpflichtungen ausgesetzt wären. Offensichtlich wurde diese Arbeit bisher nicht gemacht. Mit Hilfe dieser Arbeit kann vor allem festgestellt werden, was insbesondere im Rahmen der polizeilichen und gerichtlichen Zusammenarbeit verbessert werden muss. Auch eine Studie über die Auswirkungen könnte in Bezug auf den Einfluss der Aufhebung der Lokalisierungsverpflichtungen auf die Datensicherheit durchgeführt werden, sogar dann, wenn die Sicherheitsnormen angeglichen wurden, damit man feststellen kann, ob die physische Lokalisierung für die Datensicherheit tatsächlich keinerlei Rolle spielt.

- **Die Bedingungen für die Angleichung**

Vor der Sanktionierung des Grundsatzes müssen die Bedingungen für die Angleichung der vorhandenen Bedingungen festgelegt werden, um zu vermeiden, dass insbesondere hinsichtlich der Datensicherheit « Dumpingphänomene » auftreten. Es scheint notwendig, die Arbeit der Erfassung der nationalen Lokalisierungsverpflichtungen aus Transparenzgründen fortzusetzen und dies mit Maßnahmen zur **Angleichung der vorhandenen Verpflichtungen** zu koordinieren. Die Festlegung der Lokalisierungsverpflichtungen, welche für die Erfüllung der Aufgaben der staatlichen Verwaltung am nützlichsten sind, sollte für die Arbeit dieser Angleichung bestimmend sein.

Parallel dazu ist es notwendig, die Bedingungen für die Schaffung neuer Verpflichtungen festzulegen. Es existieren Unsicherheiten in Bezug auf die Nutzung von Daten, vor allem im Hinblick auf die Ausübung der Staatsgewalt, sowie auch bezüglich der künftigen Sicherheitsanforderungen. Daher wäre es nötig, Prozeduren für die Schaffung neuer Verpflichtungen festzulegen, die ausreichend flexibel sind, um effizient zu sein, ohne jedoch die Harmonisierung des Marktes zu gefährden.

- **Schaffung eines globalen Rahmens**

Die Einführung eines generellen Rahmens, der vertrauenserweckende Garantien für den Datenverkehr liefert, könnte daher der Aufhebung der Lokalisierungsverpflichtungen vorgezogen werden. Für die Europäische Union bietet sich jetzt die Gelegenheit, einen ausgeglichenen Datenraum zu schaffen, der als Modell für kommende Verträge über Freihandelszonen dienen könnte. Es geht darum, eine Alternative zum Grundsatz des Datenverkehrs ohne Absicherung anzubieten, indem Regeln in Bezug auf den Zugang zu Daten, deren Kontrollen und Sicherheit angeboten werden, die in der Lage sind, den freien Datenverkehr zu fördern und potentielle Implikationen im Hinblick auf die Staatenhoheit zu berücksichtigen.

[1] Da die Einführung der Datenschutz-Grundverordnung (DSGVO) den Verkehr personenbezogener Daten erleichtert, geht es bei der Einführung dieses Grundsatzes in erster Linie um den Datenverkehr bei nicht personenbezogenen Daten.

[2] Facilitating cross-border data flow, Studie der Europäischen Kommission, 2016

[3] ibidem

[4] https://www.ovh.com/fr/images/news/plan-cloud computing/rapport-cloud computing.pdf, OVH - Nouvelle France industrielle, 2014