STORMSHIELD

MEINUNGEN

# KANN ES WIRKLICH EINE EUROPÄISCHE DIGITALE SOUVERÄNITÄT GEBEN?

**Pierre-Yves Hentzen**
Chief Executive Officer,
Stormshield

**Der Begriff der digitalen Souveränität ist in politischen Reden regelmäßig zu hören. Doch in einer globalisierten Welt, in der jede Nation in unterschiedlichem Maße von anderen abhängig ist, sind die Schwierigkeiten, die es zu bewältigen gilt, um eine solche Souveränität zu erreichen, immens. So sind die Cloud-Wirtschaft, die Cybersicherheit oder auch die Beherrschung der wesentlichen digitalen Infrastrukturen zu den Herausforderungen eines turbulenten Wettbewerbs zwischen Nationen geworden, die ihre Zukunft sichern wollen. Kann Europa daraus souverän hervorgehen oder ist die digitale Souveränität nur eine Utopie?**

Im September 2021 wurde bei einem Presseabend am Rande der Monaco Assises in einem Rundtischgespräch diese Frage angesprochen: „*Die Olympischen Spiele 2024: Wie bereitet sich das französische Team auf die Herausforderungen der Cybersicherheit vor?*“ Eine grundlegende Frage, insbesondere seit den Ankündigungen des Internationalen Olympischen Komitees (IOC), das sich für die Cloud-Lösungen des chinesischen Riesen Alibaba entscheidet. Eine große Inkohärenz, sodass das Thema von **Bernard Le Gorgeu**, Sektorkoordinator für große Sportereignisse bei der französischen Behörde ANSSI, als „*sehr ernst*“ eingestuft wird. **Ziad Khoury**, Präfekt und nationaler Sicherheitskoordinator für die Olympischen Spiele, erinnerte seinerseits an die Verpflichtung des Innenministeriums, „*das französische Wissen aufzuwerten*“, und an dessen Verbundenheit „*mit der Idee der digitalen Souveränität*“.

## EINE LANG ERSEHNTE DIGITALE SOUVERÄNITÄT

Der Begriff der digitalen Souveränität taucht in Frankreich erstmals 2011 auf, und zwar unter dem Impuls von **Pierre Bellanger**, der ihn in einem Gastbeitrag definiert: „*Digitale Souveränität ist die Beherrschung unserer Gegenwart und unseres Schicksals, wie sie sich durch den Einsatz von Computertechnologien und -netzen manifestieren und ausrichten*". Seitdem blüht der Begriff in allen politischen Programmen und hat die Reden zahlreicher Minister, Staatssekretäre für digitale Angelegenheiten und sogar des Präsidenten der Republik geprägt.

Dieser Wille, die digitale Souveränität des Landes zu verteidigen, lässt sich bereits durch die Bedeutung der digitalen Wirtschaft erklären: Allein in Frankreich würde sie angeblich mehr als 6% des BIP ausmachen (fast 150 Milliarden Euro). Andererseits ist der Wunsch der Öffentlichkeit nach Unabhängigkeit extrem stark: 87% der Franzosen möchten die wirtschaftliche Abhängigkeit Frankreichs vom Ausland verringern. Aber **sollten diese Überlegungen auf nationaler oder auf europäischer Ebene angestellt werden?** „*Auch wenn dies auf nationaler Ebene geschehen kann, muss dieser Wunsch nach digitaler Souveränität durch eine gemeinsame Antwort auf europäischer Ebene und durch ein Bewusstsein bei Investitionen oder Einkäufen erfolgen*", erklärt **Florian Bonnet**, Leiter des Produktmanagements bei Stormshield. *Und bislang besteht die Strategie Europas darin, die Abhängigkeit seiner Mitglieder von außereuropäischer Technologie und außereuropäischem Kapital zu verringern, aber reicht das aus?*" Diese Ansicht spiegelt einige andere Stellungnahmen von Experten wider, die auf die **Schaffung von europäischen Champions drängen**. Davon ausgehend sollte die digitale Souveränität Europas, sollte sie eines Tages Wirklichkeit werden, durch die Schaffung dieser Champions an drei wichtigen Fronten erfolgen: Cloud, Cybersicherheit und Infrastruktur.

## CLOUD: EUROPA SCHLÄGT ZURÜCK

Angesichts des Zustands des Cloud-Marktes ist die US-amerikanische Vorherrschaft offensichtlich. Derzeit sind Amazon, Microsoft und Google zusammen 69% der europäischen Cloud, während die größten europäischen Akteure weniger als 2% ausmachen. (von denen OVH als französischer Champion gilt). Bei einem jährlichen Wachstum von 25 % dürfte dieser Markt bis 2030 ein Volumen von fast 500 Milliarden Euro erreichen ... Über das Ideal der Souveränität hinaus besteht auch die kolossale Herausforderung, die digitale Wertschöpfung nach Europa zurückzuholen.

Aber wie kann man dann die Linien bewegen? Um zu versuchen, diese Fragen zu beantworten, gab sich die EU im April 2016 die berühmte Datenschutz-Grundverordnung (DSGVO) (vor der Umsetzung im Mai 2018). Das Hauptziel des Textes besteht dann darin, die europäischen Bürgerinnen und Bürger bei der Verarbeitung ihrer personenbezogenen Daten zu schützen. Sie schafft damit aber auch einen regulatorischen Nährboden, auf dem europäische technologische Lösungen leichter gedeihen können (da sie als erste die Verordnung einhalten sollen). Und dieser Regulierungsansatz findet sich auch in der

europäischen NIS-Richtlinie (Network and Information Security) wieder. Mit ihr müssen die Anbieter von Cloud-Diensten Folgendes beachten eine Verpflichtung zur Sicherheit und mehr Garantien rund um die Datenkontrolle, die Reversibilität, die IT-Sicherheit und die Souveränität bieten. Den ausländischen Champions einfache gesetzliche Regelungen entgegensetzen? Die Idee ist jedoch in Europa nicht unumstritten, wo viele Stimmen über eine defensive Antwort der Europäischen Union alarmiert sind, wo sie doch in die Offensive gehen sollte. **Cyrille Dalmont**, wissenschaftlicher Mitarbeiter am Thomas-More-Institut, zögert nicht, die DSGVO mit einer „*Maginot-Linie*" des Digitalen zu vergleichen und ihre völlige Ineffizienz beim „*Aufbau einer unwahrscheinlichen europäischen Souveränität, deren Garant sie wäre*," hervorzuheben. Die DSGVO würde somit die europäischen Klein- und Mittelbetriebe stärker benachteiligen, da sie „*praktisch keine Auswirkungen auf die globalen digitalen Giganten hat*". Seiner Meinung nach würde Europa seither ständig versuchen, die Versäumnisse der DSGVO durch das Hinzufügen neuer Verordnungen (darunter der Digital Services Act und der Data Governance Act) auszugleichen. Diese „*normative Inflation*" würde zu einer „*tödlichen Trägheit*" führen, während die EU stattdessen „*die Bildung europäischer digitaler Champions fördern sollte*". Und sie zu schützen, nach dem Vorbild der USA und der Untersuchung der Alibaba Cloud.

Parallel zu den europaweiten Regulierungsmaßnahmen ergreifen einige Regierungen (hauptsächlich in Frankreich und Deutschland) **engagiertere Vergeltungsmaßnahmen**. Vor kurzem hat das Bundesland Schleswig-Holstein in Deutschland seine Absicht bekannt gegeben, die Nutzung des Betriebssystems Windows von Microsoft sowie alle Office-Tools aufzugeben und auf freie Lösungen unter Linux und LibreOffice umzusteigen. Die französische interministerielle Direktion für Digitales (DiNum) hat die gleiche Meinung vertreten und eine Mitteilung an alle Generalsekretäre der Ministerien versandt, um auf die Nichtkonformität von Office 365 hinzuweisen: „*Die den öffentlichen Bediensteten angebotenen Lösungen für Zusammenarbeit, Bürokommunikation und E-Mail sind Systeme, die mit sensiblen Daten umgehen. So entspricht die Migration dieser Lösungen auf das Office 365-Angebot von Microsoft nicht der Doktrin „Cloud au Centre" (Cloud im Zentrum).*"Diese Doktrin „Cloud au Centre" legt die Roadmap der französischen Regierung fest, um die Cloud „*zum Standard-Hosting- und Produktionsmodus für die digitalen Dienste des Staates*" und der öffentlichen Akteure zu machen, wobei starke Souveränitäts- und Sicherheitsprobleme enthalten sind. So heißt es dort schwarz auf weiß: „*Die Einführung der Cloud darf die Entscheidungs- und Handlungsautonomie des Staates nicht beeinträchtigen, ebenso wenig wie seine digitale Sicherheit und die Widerstandsfähigkeit seiner Infrastrukturen, die Kontrolle des Staates über die ihm anvertrauten Daten und Verarbeitungen, die Einhaltung der europäischen Vorschriften zum Schutz personenbezogener Daten, und dies zu einer Zeit, in der der Einfluss außereuropäischer Akteure im Bereich der Cloud vorherrschend ist*".

*„Sind die US-amerikanischen Interessenvertreter am besten geeignet, um zu entwickeln und darzustellen, wie eine europäische Souveränität aussehen sollte?“*

**Leonidas Kalogeropoulos,** Generaldelegierter des Open Internet Project

Doch während einige in Europa versuchen, diesen Ansatz zu übernehmen, steht dieser Wunsch oftmals **den aggressiven Lobbying-Praktiken ausländischer Akteure gegenüber. Yann Lechelle**, Generaldirektor von Scaleway, wird dem nicht widersprechen. Das Unternehmen ist einer der 22 Gründer des Gaia-X-Projekts, das den Aufbau einer souveränen europäischen Cloud zum Ziel hat. Der Unternehmer hat jedoch offiziell den Rückzug seines Unternehmens aus dem Projekt bekanntgegeben und kritisierte, dass es sich um eine Farce handele, die unter den Einfluss der USA und Chinas geraten sei. Tatsächlich waren Unternehmen wie Amazon, Google, Alibaba oder Palantir als Sponsoren eingeladen. „*Wäre es denkbar, dass ein Verband der Anonymen Alkoholiker von einem Spirituosenkonzern gesponsert wird?,* fragt Yann Lechelle. *Europa macht sich lächerlich.*“ „*Kann Europa wirklich behaupten, seine Souveränität mit der Schaffung einer digitalen NATO bis 2030 zu sichern?*“, fragte Florian Bonnet seinerseits. Auch **Jean Noël de Galzain**, Vorsitzender von Hexatrust und der Wallix Group, bezeugt die Macht des Einflusses, den GAFAM und BATX demonstrieren. In einem Gastbeitrag kritisiert er die Vereinbarungen zwischen Thales und Google Cloud „*zur Gründung eines Joint Ventures, das ein Angebot bereitstellen soll, das den Kriterien des Gütesiegels „vertrauenswürdige Cloud“ entspricht, in Übereinstimmung mit der nationalen Strategie Frankreichs*“. Dieser Kampf um Einfluss geht sogar so weit, dass er tief in die Debatten um die Definition der digitalen Souveränität selbst eindringt, von denen einige sich dafür einsetzen für einen Ansatz, der ausländischen Akteuren offen steht. In einer Pressemitteilung die Anfang Februar 2022 verbreitet wurde, fragt sich **Leonidas Kalogeropoulos**, Generaldelegierter des Open Internet Project: „*Sind die US-amerikanischen Interessenvertreter am besten geeignet, um zu entwickeln und darzustellen, wie eine europäische Souveränität aussehen sollte?*“

## CYBERABWEHR: FRANKREICH WILL EUROPA AUF VORDERMANN BRINGEN

Diese Doktrin „Cloud im Zentrum“ ist auch ein Symbol für die **Konvergenz von Cybersicherheit und Cloud**, da sie es zwingend erforderlich macht, dass digitale Produkte, die mit sensiblen Daten umgehen, „*in der internen Cloud des Staates oder in einer durch die ANSSI als SecNumCloud qualifizierten kommerziellen Cloud gehostet werden*“.

Diese Konvergenz ist nicht unbedeutend. Denn wenn Europa überhaupt die angestrebte digitale Souveränität erreichen will, muss es dafür zweifellos in der Lage sein, diese zu schützen. Nun hat **Margarítis Schinás** auf dem Internationalen Forum für Cybersicherheit, das im September in Lille stattfand, die Befürchtungen der höchsten

europäischen Instanzen in Bezug auf die Cyberabwehr ausführlich kommuniziert. Die Vizepräsidentin der Europäischen Kommission beschrieb „*eine kritische Situation*“ und die „*jüngste Vervielfachung von Cyberangriffen durch internationale Akteure*“, die **dramatische Auswirkungen auf die öffentlichen Dienste und damit auf die Stabilität Europas** haben würden. Frankreich, das den Vorsitz im Rat der Europäischen Union übernommen hat, hat bereits mehrfach seine Absicht geäußert, die EU umzustrukturieren, um sie mit angemessenen Cyberabwehrkapazitäten auszustatten. Auf europäischer Ebene möchte Frankreich nicht mehr von Cybersicherheit, sondern von Cyberabwehr sprechen. Die Herausforderung wird militärisch, wie der Beitrag der französischen Verteidigungsministerin **Florence Parly** zeigt, die sich fragte, ob es sich um ein Wiederaufleben „*eines Kalten Krieges im Cyberspace*“ handele. So kündigte Frankreich die Verstärkung seines Kontingents für die digitale Kriegsführung an und möchte auf diese Weise „***ein europäischer Champion der Cybersicherheit***“ werden. Mit dem Ziel, die gesamte Europäische Union dazu zu bringen, ihre Verteidigungsfähigkeiten auf die gleiche Weise zu strukturieren.

Während solche Reden deutlich machen, wie ernst die Cybersicherheit bei der Verteidigung der europäischen Souveränität genommen wird, strukturiert sich Europa derzeit mit neuen Gesetzestexten ... So diskutieren das Europäische Parlament und der Europäische Rat derzeit über die Überarbeitung der Richtlinie NIS 2 (Network and Information Security), die die Liste der sensiblen Sektoren erheblich erweitern soll. Während die Liste der Betreiber wesentlicher Dienste (ESO) bisher im Ermessen der Mitgliedstaaten lag, wird die Richtlinie NIS 2 (Network and Information Security) die Kriterien dafür vorschreiben, indem sie zu den bereits einbezogenen Bereichen (wie Banken, Energie, Gesundheit usw.) neue Sektoren hinzufügt (Postdienste, Abfallentsorgung, großer Lebensmitteleinzelhandel usw.). Ein weiterer wichtiger Punkt ist, dass zentrale und staatliche Verwaltungen offiziell in den Geltungsbereich der Richtlinie fallen und zu Betreibern wesentlicher Dienste werden, während das Hinzufügen von regionalen und lokalen Verwaltungen weiterhin den Mitgliedstaaten überlassen bleibt.

## INFRASTRUKTUR: EIN STILLER CYBERKRIEG

Während die Cloud und die Cybersicherheit die sichtbaren Säulen der digitalen Souveränität sind, gibt es eine dritte, die weniger das Interesse der breiten Öffentlichkeit auf sich zieht, obwohl dort ein regelrechter Hegemonialkrieg stattfindet: die Infrastruktur.

Im Juni 2019 warnte die Interministerielle Direktion für digitale Angelegenheiten (Dinum) bei einer Anhörung vor dem französischen Senat: „*Wenn wir nicht über Akteure verfügen, die in der Lage sind, die Infrastruktur zu produzieren, die Dienste zu bauen, die Beziehung zu den Nutzern auf der ersten Ebene zu verwalten und die Schnittstellen zu beherrschen, werden wir in Sachen Souveränität wahrscheinlich in die zweite Liga absteigen*“. Im August desselben Jahres verabschiedete die Versammlung ein oft als „Anti-Huawei-Gesetz“ bezeichnetes Gesetz, das die Genehmigungen für ausländische Wirtschaftsakteure zur Unterstützung und zum Betrieb von Mobilfunknetzbändern erheblich einschränkte.

Auch wenn das Ziel nicht gleich zugegeben wird, sollte dieses Huawei-Gesetz und jeden anderen chinesischen Akteur aus dem Rennen um die Installation der Netzinfrastruktur ausschließen, die als Grundlage für das künftige französische 5G-Netz dienen wird. Damit folgte Frankreich Großbritannien und Schweden (ganz zu schweigen von den USA unter der Trump-Regierung), die alle ähnlich vorgegangen waren. Eine Stellungnahme, die sich nahtlos in die defensive Politik der EU und ihrer Mitglieder in Bezug auf die Souveränität einfügt.

Doch dieser Infrastrukturkampf wird nicht nur um die Wellen geführt, sondern auch im Meer. Derzeit werden 99 % der interkontinentalen elektronischen Kommunikation über Unterseekabel abgewickelt. Im Sinne der Souveränität muss die Europäische Union sicherstellen, dass diese Infrastrukturen nicht unter die Kontrolle ausländischer Einrichtungen fallen. Da dieser Sektor jedoch kaum reguliert ist (eben aus der Logik der staatlichen Neutralität heraus), drängen sich private Akteure aus der ganzen Welt, um sich die Kontrolle zu sichern. Die US-amerikanischen GAFAM, die traditionell als Konsortium von Telekommunikationsbetreibern (viele davon aus Europa) fungierten, sind im letzten Jahrzehnt mit unvergleichlicher Stärke ins Rennen gegangen. **Jean-Luc Vuillemin**, Leiter der internationalen Netzwerke von Orange, konstatiert die erschreckende Entwicklung in einem Interview: *„vor zehn Jahren wurden 5% der Unterseekabel von den GAFAM kontrolliert. Heute sind es 50 % und in den nächsten drei Jahren werden es 95% sein“*. Dieser Entrismus der großen amerikanischen digitalen Plattformen, die von den chinesischen BATX nachgeahmt werden, hätte den Sektor in einen *„wahren Wilden Westen“* verwandelt, in dem das Recht des Stärkeren über das gemeinsame Interesse gestellt wird.

Der Befund ist klar: Von seiner infrastrukturellen Basis bis hin zur Wertschöpfung **ist der digitale Bereich Europas noch weit davon entfernt, souverän zu sein, und wird jeden Tag mehr und mehr von außen unter Druck gesetzt**. Auch wenn der Begriff der digitalen Souveränität ein sowohl wirtschaftlich als auch geopolitisch verständliches Ideal ist, scheint die Europäische Union derzeit den Weg der Überregulierung zu wählen. Bevor Sie einen Gang höher schalten? Dies ist zumindest das Signal der Europäischen Kommission, die gerade, ganz am Anfang des Jahres 2022, einen Aufruf zur Einreichung von Projekten in Höhe von 80 Millionen Euro gestartet hat, um die Einrichtung eines europäischen DNS-Auflösungsdienstes zu fördern.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**