European Public Goods

Vision Europe | July 2020

Digital Sovereignty in the EU

Falk Steiner and Viktoria Grzymek

“Digital Sovereignty” is a term frequently used in political debates on the national and European level. What is meant by this? How can the EU be capable of asserting its own values and legal systems in a digital policy?

The debate on “Digital Sovereignty” is not sufficiently based on evidence at the present time. To date, there has been a lack of both concepts for ascertaining Germany’s and the EU’s actual degree of dependence on third countries and the political desire to determine this. This means that a conceptual response to the problem of dependence is also missing. Nonetheless, Europe is still in a fundamentally better position than it was a few months ago – and does not necessarily have to face the issue on its own.

This article initially addresses the background and evolution of digitalisation, then outlines Digital Sovereignty as a concept for the European Union and lays out an approach for identifying and judging dependencies. The last part of the article describes possible derived steps to be taken and the framework conditions for a digitally more sovereign European Union and the conditions to be established for this within the EU.

If European competencies and common goods are considered in the context of digitalisation, it is necessary to start by stating two aspects that need not be discussed further:

1. Europe already has a Digital Single Market today, and it has also continued to work during the Coronavirus period.
2. Individual EU Member States in and of themselves are to be considered too lightweight for any form of Digital Sovereignty.

BertelsmannStiftung

The latter point shapes the character of Digital Sovereignty as a public good that is necessarily handled on the European level – solely in the framework of the EU do the Member States have the market and regulatory influence allowing for the design of digitalisation according to their own standards and values.

At the same time, many aspects of the debate on Digital Sovereignty should also be applicable to other areas where for strategic reasons it appears urgently necessary to have and build up the EU's own capacities and competencies, rebalance dependencies and introduce a more conscious state of globalisation.

Europe's ability to act under the pressure to digitalise

Europe and the digital world – this has often been more a random tragedy than a systematic policy in recent years. An understanding, defined specific goals, and competencies are all lacking.

Yet digitalisation itself is critical for what is considered European: In partially globalised societies and public spheres, this technology is the power directly affecting all of our lived realities – much more directly than laws or moral conceptions, European constitutional conventions or councils of ministers. Both consciously and unconsciously, technology is always perceived according to the values of the respective regional context in which it is developed and deployed. This applies whether it involves the private sphere, the reliability or unreliability of contents, access possibilities for government actors or the treatment of individual citizens.

In digitalisation, technologies and their respective application must reject the real-life assertion of values such as right, wrong and desirable – for example, when it comes to restrictions on freedom of expression in the digital public sphere. Values and norms in the digital world change when they are implemented technologically, implicitly or explicitly, and they cause a very real-life change in the understanding of values in societies as a result of the repercussions of this implementation. In turn, this is reflected in contemporary values and the interpretation of the canon of values.

Digitalisation is defined by the following characteristics: In the West, it is largely handled by private actors and is thus characterised by global contractual relationships in the private sector, although the legal framework for effective enforcement in this regard is often lacking. There is no notable public sector in the digital sphere; there are only publicly accessible areas, i.e. services and products that are usually provided by the private sector. However, the pressure for politicians to act is increasing – which is why a new policy field has developed, one that is both independent of all other areas and simultaneously penetrates almost every one: digital policy.

Digital policy: colliding worlds

Digital policy is a field with two sides. One addresses the existing original digital world, essentially the resources of the digital society. Examples of this include the digital infrastructures such as broadband networks, mobile networks, nodes, computer centres and digital services as well as their security. Yet it also consists of the political-legal, economic and social regulatory mechanisms, technological-architectural framework conditions and the implicit normative assumptions that have developed in the creation of digital products and services (mostly defined by the West).

The other side of digital policy involves those areas that have been significantly changing due to digitalisation – which makes this change the subject matter of digital policy. This begins with intangible assets such as classical intellectual property rights or competition policy. Yet it also covers issues related to the enforcement of law in the digital sphere, for example, in the case of illegal content according to nation-state criteria, the handling of newly created dependencies in the digitalisation of (partially) autonomous vehicles or in agriculture. Finally, it takes up the basic question of how it is politically, legally and socially possible and advisable to adequately levy taxes and duties in the case of highly automated added value.

Both areas are closely connected with each other, but suffer from two opposing problems of perspective: The original digital world has developed as an autonomous area over the last 50 years, largely ignoring older established models of government regulation and inter-state coordination, yet the digitalising areas are entrenched in their respective contexts, which are then severely hit by some aspects of digitalisation and new actors at regular intervals. Over the last 25 years, this can be seen in the example of mail ordering (Amazon and AliBaba Express vs. Neckermann, Quelle), the music industry (Streaming and MP3 vs. single CDs), television (Netflix vs. ProSieben), new mobility providers (Uber and Lyft vs. taxi industry), the renting of temporary office space (WeWork vs. Regus), food delivery services (Lieferando vs. Call-a-Pizza), information organisation (Brockhaus and Encyclopedia Britannica vs. Wikipedia) to the role and responsibilities of telecommunications companies (WhatsApp vs. SMS) and many other examples.

Even if we avoid the grandiloquent word disruption, there are still massive structural changes in entire industries and enormous changes in business models and value-added chains that are in part based on the two factors of scaling and network effects (up to and including natural monopolies) in all markets that can be accessed technologically, economically and culturally. However, the access conditions are very different, also on account of the origin of the actors – and political reasons account for this to some extent.

Digital policy as a government policy field

USA: the world as market for technology and liberalism

In the USA, the strategic relevance of the digital sphere was recognized and promoted at an early stage. Logically after the deregulation of the telecommunications market, it was understood primarily as a vehicle for the global spread of the liberal world order and a corresponding global economic system – e.g. by then US Vice President Al Gore, who pursued the strategic digital policy in the 1990s. To date, the fundamental view of digitalisation as a positive development has hardly changed despite different presidencies. In the USA, furthermore, there has also been a long tradition of private and scientific actors on the one hand and the military or intelligence community on the other working to advance technological development and use. In parts of Europe, these participants do not necessarily work together as closely, and often this is expressly not desired. The USA has focused on three major political-strategic areas: (1) creating an attractive environment for innovation with adequate capitalisation options within the USA, (2) keeping markets open through international treaties with the (3) simultaneous commitment to securing every kind of intellectual property and the greatest-possible cybersecurity, both offensively and defensively.

China: the state regulates the domestic market

China largely missed out on the first years of networked digitalisation. In the 2000s, however, there was a clear rethinking as industrialisation moved ahead: While mainland China initially became a technology production site, especially with highly welcome US and Taiwanese companies in the semiconductor industry, this was accompanied by the development of its own competencies. Chinese politicians' specific openness to technology plays a major role here: The Communist Party of China (CPC) recognized that growth in traditionally industrial sectors is finite and that other countries had a huge head start. However, the evolving digitalisation offered two opportunities simultaneously: greater opportunities for surveillance and control domestically as well as the systematic promotion of the economy.

Starting in 1997, China began to monitor internet connections in the People's Republic, subject them to censorship (2003 "Golden Shield") and ensure the separation of the Chinese internet through the Great Firewall of China. Strict requirements for foreign direct investments, which usually only allowed market access to companies that created joint ventures with Chinese partners, also let the People's Republic secure its own major interests. Foreign partners often abandoned the difficult market some time after the unequal conditions were used for the advantage of the Chinese participants.[1]

At the same time, China became an increasingly attractive market due to its own citizens' increasing purchasing power and profited greatly from the development of competency and access to technologies from other countries, while the state also massively subsidised its own digital ecosystem: The CPC's ideology views technology as an opportunity to enforce its specifically interpreted public welfare interests and has repeatedly admitted to real experiments on population surveillance and control in test regions.

This combination of a closed public sector, closed market, massive research investments and state subsidies has also been supported by a systematic export policy in recent years. The nontransparency of Chinese state subsidies continues to result in global distortions, with China massively exporting total package technologies to foreign countries as part of its global activities and establishing structural dependencies on Chinese suppliers there.

Europe: hesitant, but slowly waking up

The EU massively underestimated the scope of digital developments. After the first establishment of the framework in the 1990s and the cautious adjustments in the following years, especially the Member States with national success and strategies viewed themselves as sufficiently equipped to sail towards an information society in the wake of the US-dominated developments.

And for a long time, this also appeared to go well: Nokia achieved a share of almost 50 percent of the global mobile phone market in 2007, primarily threatened by the Canadian manufacturer Research in Motion and its Blackberry business smartphones. But Apple's iPhone led to a completely new type of mobile phone and by the beginning of 2012 Nokia's market share had slipped to 7.8% and has not recovered since then. The famous Nokia ringtone, the "sound of market power", turned into the sound of decline. It was a fate that befell other, temporarily successful manufacturers in this sector, from Siemens to Motorola. However, the shift can also be seen in the much younger smartphone market: the actual innovations came from North America; the products were manufactured in the People's Republic of China, and after some time the European suppliers could no longer keep up – but Europe remained one of the most important sales markets.

Meanwhile, the efforts to shape the Digital World in Europe were narrowed down even further to the question of whether change was really necessary, whether more Europe was really necessary in this area; for example, it was questioned whether the Single Market truly needed a digital equivalent. Debates on the 'right' digital policy were largely limited to the questions of telecommunications market regulation, copyright, cybercrime and increasingly surveillance and a continental European understanding of data protection. However, it took until the outrage and debate over the potentially massive access of US intelligence services following the publications on the basis of the Snowden archives for broader, more fundamental, strategic considerations to be made on the extent to which dependence on third parties had exceeded a permissible and reasonable scope. This had immediate consequences for the question of whether and to what extent Europe had an obligation to protect in the digital sphere beyond a mere territorial principle and whether the existing deficiencies in law enforcement could be remedied.

International: the primacy of the digital world?

Major actors in digitalisation do not reside in the Member States of the EU – which means that European law cannot be enforced per se with respect to them (see Figure 1).

Even inside the EU (1,2,3), there are already considerable differences in the legal treatment of matters – and the underlying regulatory system can differ substantially between countries, for example as to whether preventive or follow-up concepts are pursued. The "Digital Single Market" continues to exhibit major differences – i.e. in tax treatment or media regulation.

[1] These conditions were only loosened somewhat in early 2020 and after increasingly loud criticism ("Foreign Investment Law"), but direct investments in China continue to be subject to some otherwise unusual restrictions.

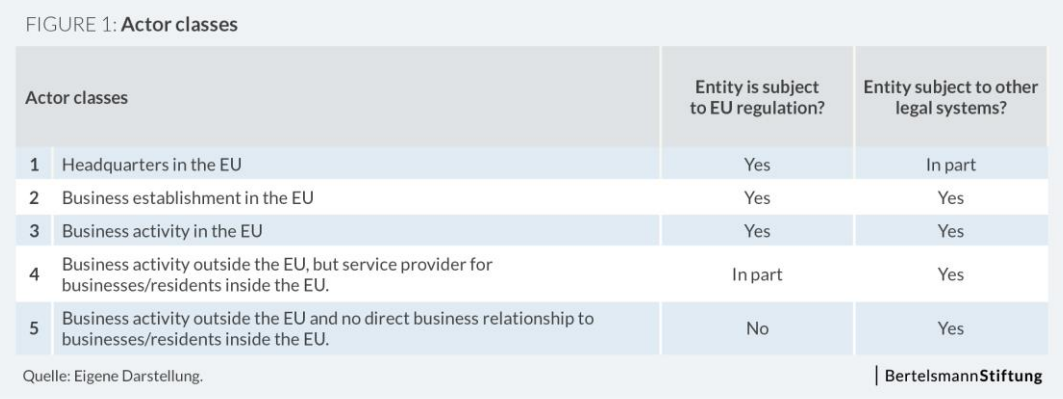

FIGURE 1: **Actor classes**

	Actor classes	Entity is subject to EU regulation?	Entity subject to other legal systems?
1	Headquarters in the EU	Yes	In part
2	Business establishment in the EU	Yes	Yes
3	Business activity in the EU	Yes	Yes
4	Business activity outside the EU, but service provider for businesses/residents inside the EU.	In part	Yes
5	Business activity outside the EU and no direct business relationship to businesses/residents inside the EU.	No	Yes

Quelle: Eigene Darstellung.

| BertelsmannStiftung

Fundamentally, the country-of-origin principle applies in the EU: the law of the country in which a company has its headquarters is authoritative. However, this does not apply universally: If consumer contracts are concluded (e.g. on user accounts and general terms and conditions), the application of European consumer contract law is mandatory – independently of the headquarters of the supplier. Nonetheless, law enforcement in many cases is not practically possible, e.g. with respect to Chinese suppliers. Law can be enforced with respect to such companies if they have business establishments inside the EU.

The form of the so-called “virtual business establishment” is uncharted territory for regulation. At least in terms of tax law, this type of establishment should include companies that do not operate a classical business establishment, but do business on the EU market (3). A “significant digital presence” in the EU for this would be used as the criterion for the tax treatment of sales revenues and profits in the EU.

However, the EU also ventured into uncharted territory with the General Data Protection Regulation (GDPR): It applies to all classes from 1 to 4 and is tied specifically to the business – irrespective of a company’s headquarters, for the most part: If personal data on citizens residing in the EU is processed (also on a contract basis) in order to observe their behaviour or offer them services and goods, the company is subject to the regulatory framework of the GDRP. This offers the possibility of classifying the legal framework of the country of origin as guaranteeing an adequate level of protection. It involves an extension of the market place principle, which goes beyond the EU’s own borders – an expression of Europe’s Digital Sovereignty? One debate illustrates the difficulties to date.

The 5G debate: Europe makes life hard for itself

At the beginning of 2015, there was one goal: make mobile data available everywhere in the EU as quickly as possible. What followed was a prime example of European digital policy: The Member States managed to coordinate the necessary frequencies within Europe – but that was almost all that the European community agreed on. 28 Member States introduced frequency requirements in national procedures. 28 times, different conditions were imposed. And 28 times, the respective requirements for the telecommunications providers differed. As if that wasn’t enough, the issue of the fundamental trustworthiness of Chinese network suppliers – with the Chinese companies Huawei and ZTE being two of the five global suppliers – also moved onto the political agenda in the course of the trade disputes between the USA and China.

In Europe, too, there had already been criticism that the EU might be overly dependent on Chinese suppliers, given the expected importance of 5G as an integrated network technology from private households to intelligent sensor technology on the streets, roads, bridges, factories and the role of technology for automated and autonomous vehicles. However, after the US decision to exclude Chinese suppliers and rely primarily on the two European suppliers, Nokia and Ericsson, Europe was under massive pressure from its transatlantic ally to block Chinese suppliers from building the 5G infrastructure.

The debate centred on three scenarios: firstly, the fear that Chinese companies could be obliged to participate in espionage activities under the law of the People’s Republic and that these activities might remain undetected and untraceable. The second fear revolved around the so-called kill-switch scenario, a special form of sabotage: Chinese actors could switch off individual network segments or even entire networks by remote maintenance. The third scenario, by contrast, was more of an industrial policy issue: If Huawei and ZTE were to serve the European market, there would be a medium-term threat that the other suppliers would disappear and the EU would be completely dependent on foreign companies, which in turn could make scenarios 1 and 2 even more likely. One special aspect in the debate was the question of how close the companies are to the state leadership in Beijing – this question was never conclusively answered in fact, but such large companies are in principle hardly viable in China without being close to the CPC.

The whole debate revealed Europe's weaknesses: it started far too late, the Member States tried to solve the problem individually and only a few pressed for a joint solution, while Chinese representatives – both members of the diplomatic corps and non-diplomatic company representatives – lobbied individually in each Member State, declaring the problem non-existent and pointing out the possible consequences of excluding Chinese suppliers, also for the business activities of Member State companies in China. Only three quarters of a year after the beginning of the debate was it possible to agree on specific proposals from Brussels in January 2020: the so-called "5G Toolbox", the toolbox for fifth generation mobile communications. The content of this toolbox is little more than an emphatic appeal to Member States that they comply with uniform minimum standards.

However, there has also been a positive side to the 5G debate for Europe: awareness of the massive dependencies in the digitalisation of problematic actors has increased significantly, coupled with the realisation that the usual reactive and national approach cannot adequately address such problems. This is one of the main reasons why a new objective must be adopted: Digital Sovereignty.

In the confusion: Digital Sovereignty cannot be binary

The term Digital Sovereignty has become enormously popular, especially in the last few months, and familiarity with it has been amplified by the postulated ambition of a geopolitical commission. Many of the aspects discussed are not necessarily specifically digital, but must also be taken into account in other fields. In political speeches and catalogues of requirements, it is a regular part of the debates surrounding the 5G network equipment suppliers or in the context of the data strategy of the EU Commission, whose concept of common data spaces should improve "Europe's technological sovereignty in key technologies and infrastructures for the data economy",[2]which is expressed with exactly these words in the whitepaper on artificial intelligence.[3] The industrial strategy of the EU Commission from March 2020 also adopts a specific sovereignty term: "Europe's digital transformation, security and future technological sovereignty depends on our strategic, digital infrastructures."[4]

The term "Digital Sovereignty" is interpreted very differently. But hardly any politician, hardly any public institution defines this term in reality. Chancellor Angela Merkel understands Digital Sovereignty to be:

> "...not protectionism or regulations by state authorities on what information can be shared – i.e. censorship –, but [...] the ability, as an individual, a single person, a society, to be able to shape the digital transformation in a self-determined way. [...] This means we need sovereignty over what happens. That is why it is also an expression of sovereignty to advocate a common, free, open and secure global Internet when we are convinced that isolation is not an expression of sovereignty,

[2] EU Commission: Europäische Datenstrategie, p. 5; Brussels, 20 February 2020 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

[3] EU Commission: Weißbuch Zur Künstlichen Intelligenz, p.3; Brussels, 19 February 2020 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.

[4] EU Commission: Eine neue Industriestrategie für Europa; Brussels, 10 March 2020, p. 13 https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf.

> but that we must have an underlying common understanding of values."

Annegret Bendiek and Martin Schallbruch provide one of the few specific definitions in their SWP article entitled "Europas dritter Weg im Cyberraum" ["Europe's Third Way in Cyberspace"][5]:

> The term Digital Sovereignty refers to the ability of a subject under international law to control and manage cyberspace.

This legal-technological perspective is a good starting point, but does not go far enough. For instance, what is "control and manage cyberspace" if one looks beyond cybersecurity and examines supply chains, intertwined services and other interdependencies?

Therefore, it is necessary to have another definition of Digital Sovereignty. A working proposal would be:

> Digital Sovereignty is the ability of an entity to personally decide the future form of identified dependencies in digitalisation and to possess the necessary powers.

This entails the following prerequisite: In order to decide personally, concrete dependencies must be recognised, analysed and evaluated, while one's own abilities and possibilities for action must be identified – in a formal as well as an actual perspective. What competencies are necessary for this? Which ones are formal and which ones are really present? If they are lacking, is it possible to create them realistically? Over what time horizon? How does one handle problems in the meantime?

In addition, there is the structural difficulty of differentiating digital capacity from other capacities such as decision-making and acting when digitalisation impacts large parts of the overall social fabric and the economy.

That is why it is necessary to start by defining which areas can be considered as not critical for the most part and which ones should be subject to conceivable, structural restrictions in the exercising of Digital Sovereignty – if this appears sensible at all, given the degree of networking with digital products and services.

This fundamentally goes far beyond the area of "Critical Infrastructures" in the sense of cybersecurity (energy, water, telecommunications, food, finance, media and transport), where criticality is defined either by the quality of the supply units or on account of the particular importance for supply.

If Digital Sovereignty in the sense of an individual's own ability to make decisions and take action is the goal, then not only the criticality of the individual product or service at the current point in time is decisive, but also the criticality of a product or service at a later point in time and in its global overall context. By no means is it sufficient to provide an answer in the binary form of dependence = yes or no. Rather, it involves granular, possibly problematic structures of dependencies on multiple levels and from different perspectives where their assessment in turn requires yet another differentiation as can be seen in the following section.

Existing dependencies: feeling about in the dark

There have been no convincing empirical studies on Europe's actual dependencies in digitalisation to date. This is quite surprising given the volume of the political arguments in this area – although by no means are many aspects of the debate new.

Essential for the question of Europe's dependencies are all areas of digitalisation where significant parts of them depend on process steps that are largely not subject to intra-European decision-making authority.

It is necessary to differentiate between two levels here: Firstly, those parts of processes that take place outside of Europe and are thus logically subject to the area of influence of others as a rule. Secondly, all steps in the process – whether taking place in Europe or other territories – that are to be assigned largely to the power or the

[5] Bendiek, Annegret / Schallbruch, Martin: Europas dritter Weg im Cyberraum. The article on the new cyberspace regulation, p. 7; Berlin, 11.2019 https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A60_bdk_Schallbruch_WEB.pdf.

decision-making authority of other, non-European actors. Steps in the process are considered to be all individual components (hardware, software, necessary infrastructures, staff, if applicable) in their manufacturing, operation and servicing and in the interaction of these steps, and may even include their individual product components and the conditions of their origin. Here again, different criticalities are to be defined: Just because steps in the process fall within the control of non-European third countries, they are not per se problematic; this depends on the respective circumstances.

A graduated approach is called for with special consideration given to the question of what values Europe shares with the respective third country and how stable this relationship is. Norway, Canada, Japan, Israel, the USA, South Africa, Brazil, India, Russia, Saudi Arabia and China are on very different levels, also in terms of digital dependence, ranging from close partnership and cooperative trade relations to destructive competitors and system rivals.

To determine specific dependencies or needs for action, it is necessary to determine the status quo in a structured manner.

- The status quo must then be broken down into the "**how**" of the specific dependence(ies) on the basis of a system of acceptability: Is the respective step in the process
    - of minor or major importance for availability, security or future dependence?
    - also fundamentally performable by others (diversification and substitution potential)?
    - competing with intra-European actors? If yes, who actually controls this?
    - unlawfully promoted by political decisions of non-European actors?
- Furthermore, the "**for what reason**" of specific dependence(ies) must be broken down: Is this due to
    - resources
    - price advantages
    - market sizes
    - subsidies
    - technological head start
    - …?

In order to be able to realistically assess the relevance of these dependencies, it is imperative to adopt a differentiated view: Are there areas in which these actors are in turn largely dependent on intra-European process steps, services and products? How resilient are the suppliers or producers to the undesirable influence of third parties (e.g. takeovers, acquisition of shares, own dependencies)?

On the basis of the status quo determined in this way, a strategic dependence management instrument could be developed in a qualified manner, which may in turn be followed by suitable legal instruments (presumably mainly commercial and competition laws).

Understanding dependencies: case analyses are the basis

To understand the complexities described here, it is necessary to analyse services and products and their intermediary goods as well as the required operating conditions and observe them and their impact collectively. It is important to work with a broad definition of digitalisation. A – by nature – still very simplified example is provided below to illustrate the arising questions. If one systematically pursued it to the end, one would have to check the supply chains all the way to the raw materials in the case of components and process parts – unless they can be substituted in their entirety.

The *supply of food* is already part of the *critical infrastructure* today since supplying the population with basic foodstuffs is absolutely necessary. The starting point for the supply here is the manufacture of a product; let us assume it is potatoes. They are sown, cultivated and harvested with modern methods on agricultural fields. The large agricultural machines usually used for this are highly digitalised products. Under the assumption that it is absolutely necessary to ensure the supply of potatoes, these machines must be checked in terms of their digital operating security. We use a simplified testing system for a closer look at the complexity of potatoes:

- Who manufactures these machines? From what components? Where are they manufactured?
    - East Westphalian agricultural machinery manufacturer

- Hardware is sourced from German and US manufacturers, IT components are produced in the People's Republic of China, Taiwan and South Korea, raw materials come from Europe, China, USA and South America.

- Who has decision-making authority over the manufacturer?
  - Joint stock corporation, 60 per cent family owned, 40 per cent owned by other investors, of which 10 per cent are non-European investors.
- Where do the software and data for the operation of the machines come from (motor and machine control, sensor control)?
  - Motor control: operator's own software development
  - Machine control: software supplied by large service providers from the UK; the software is developed in India, and the quality assurance is handled in the USA.
  - Sensor control: sourced from German manufacturer; development and maintenance in Japan
- Who is responsible for its maintenance/servicing?
  - ➢ Service Level Agreement (SLA) with manufacturer
- Is the product standardised and are its parts possible to substitute with others in the short term?
  - Parts of the product are standardised.
  - Substitution of hardware is possible in part.
  - Substitution of software is currently not possible for legal reasons (SLA) / technical reasons (code only known to the current software provider).
- Summary:
  Who has the actual decision-making authority (software, hardware) over the machine?
  - Quality assurance team for software development in the USA
  - Owner family in Germany
- Appraisal of circumstances: Is it necessary to assume that the supplier will operate in a reliable, stable legal and political framework for the foreseeable future?
  - No, because the Chinese legal system is not an independent legal system, but an instrument of political will.
- Is it to be assumed that the supplier will fall under the influence of problematic actors in the foreseeable future?
  - Yes.

This improvised, cursory test shows: Whether or not there are potatoes in Germany is not necessarily decided by the farmer or agricultural machinery manufacturer at the present time.

Let us ask the same questions about German telecommunications network suppliers and the building of the 5G infrastructure:

- Who is the supplier of the pieces of hardware used? Where are they manufactured? From what components?
  - Hardware: Chinese supplier Huawei
  - Production of IT components in the People's Republic of China, Taiwan and South Korea
  - Raw materials from China and South America
- Who has control over the manufacturer?
  - Huawei: Chinese Limited (no information about the ownership structure)
- Where do the software and data for the operation of the equipment come from (radio network, distribution networks, control elements)?
  - Software distribution networks – Cisco
  - Software control elements – open source
  - Software radio network of Chinese manufacturers
- Who is responsible for its maintenance/servicing?
  - Service Level Agreement (SLA) with manufacturer
  - Service Level Agreement (SLA) with service provider
  - Self-servicing
- Is the product standardised and are its parts possible to substitute in the short term?
  - Parts of the product are standardised.
  - Substitution of hardware is possible.
  - Substitution of software is currently not possible for legal reasons (SLA) / technical reasons (code only known to the current software provider).
  - Substitution of software is possible.
- Summary:
  Who has actual control over the equipment (software, hardware) today?
  - Quality assurance in China

  - Ownership in China
- Appraisal of circumstances:
  Is it necessary to assume that the supplier will operate in a reliable, stable legal and political framework for the foreseeable future?
  - No, because the Chinese legal system is not an independent legal system, but an instrument of political will.
- Is it to be assumed that the supplier will fall under the influence of problematic actors in the foreseeable future?
  - Yes.

This superficial test already shows the many different levels on which problems would exist and which would have to be considered in an informed decision on the aspect of digital sovereignty.

Such analyses are possible and expedient for almost all areas where digital technologies are used when it is necessary to systematically document dependencies for the first time.

The question of deciding whether there are external dependencies is accompanied by a second dimension: the question of Europe's ability to act vis-a-vis foreign countries and internally. This is largely determined by the extent to which Europe's own structures are capable of penetrating and shaping digitalisation according to European requirements in terms of content, economics, regulation, as well as executive and political policy.

It is necessary in turn to differentiate between the following here:

- the possibility of creating policy and enforcing law on all four levels, i.e. on the level of the EU, the Member State, federal state and municipality through adequate assignment of legal, institutional and staff competency (policy)
- the possibility of enforcing law through public bodies (regulatory and investigative authorities, courts)
- the possibilities for law enforcement by private parties (citizens, companies and public welfare organisations)
- the actual setting of standards in technical standardisation bodies and the international (legal) framework conditions in agreements and organisations
- the feasibility of implementation by private sector actors on the market (profitability)
- the ability of buyers and consumers to make conscious decisions (decision-making sovereignty)

The goal: a common European strategic dependence management

Much is to be said for assuming that Digital Sovereignty, as a task for society as a whole, should be closely coordinated across Europe, probably even centralised in the best case scenario, for the EU to shape digitalisation in a way that considers European values and preserves European basic principles. This is due alone to the fact that on account of the international dimension of the problem the best-performing national digital policy, even in the large European states, appears unsuitable for negotiating as equals with the actors who currently play the most important role here.

However, this would require a clear mandate – and the systematic pursuit of these goals, especially due to the cross-sectional application of digital policy in almost all other areas of policy, would come close to achieving an at least temporary full integration of the necessary competencies, which is illusory from a realistic point of view. At the same time, most Member States have become painfully aware in recent years that their own negotiating position is insufficient. The geopolitical dimension of digital policy could be a lever to review the willingness to embark on further integration limited in terms of time and scope.

Internationally, an integrated European approach would offer great opportunities: major parts of Western-style democracies (namely most OECD countries) are by no means inclined to subject themselves to the technological and thus political influence of China. However, the pure lack of serious alternatives coupled with China's very skilful digital strategy in foreign trade is currently a seemingly insurmountable hurdle for many. However, critically assessed countries such as China are not looking for massive confrontation since this would run counter to their own, primarily internal economic interests, which the EU and its Member States must consider in their actions.

The goal of such measures would have to be a joint European strategic dependence management. The first step would be to identify the existing and expected future dependencies and then in the second step to classify these dependencies and prioritise them according to criticality and mitigability. In the third step, the EU could use the goal of expanding its own abilities, consciously choosing or accepting dependencies or tolerating irrelevant dependencies to work towards strategic balances or even to possibly achieve overweights in the long run, which would once again expand Europe’s own room for manoeuvre.

The EU must also assume the position of being able to assert its own values and legal systems actively with respect to parties that do business in the European Union, but are based in third countries. And it must also reinvent its own role as an EU viewed positively by its citizens. Reviewing individual actors such as Huawei or ZTE on a case-by-case basis does not appear to be a sensible strategy in the long run since this would not rule out the spontaneous development of substitution possibilities for problematic actors – this would be considered man-to-man marking in football. Instead, zone defence must be the goal: Europe must put itself in the position of making other actors in digitalisation at least as dependent on its participation as Europe is on theirs.

Falk Steiner was a senior expert on digital policy in the Bertelsmann Stiftung’s Megatrends program from March 2019 to May 2020.

Viktoria Grzymek is a project manager in the Bertelsmann Stiftung’s “Ethics of Algorithms” project and focuses on the sociopolitical effects of algorithmic systems.

Picture: Shutterstock / maradon 333

Address | Contact

Katharina Gnath
Senior Project Manager
Program Europe’s Future
Bertelsmann Stiftung
Werderscher Markt 6, 10117 Berlin
Tel: 030 275788-128
katharina.gnath@bertelsmann-stiftung.de
www.bertelsmann-stiftung.de/europe