Chapter 10. A new age of digital trust

Francesco Bonfiglio
CEO Diagrammatica and ex-CEO Gaia-X
DOI: 10.54103/milanoup.180.c275

10.1 Digital, this great unknown

Many now recognize the significant overlap between technology, economics, and politics, but few fully understand it. The reason lies in the lack of a common knowledge base, and in the complexity of the ways in which this becomes entrenched creating dependencies in the real world, in the economy, in the political action, and in our everyday lives.

Today, digital sovereignty is seen as a crucial legal initiative aimed at reclaiming market share from a handful of dominant American companies, often referred to as GAFAM - a term that originally stood for Google, Amazon, Facebook, Apple, and Microsoft, but has since evolved to include new entrants and rebranded entities. We search spasmodically for a single solution, identifying from time to time a single problem affecting the digital world: digital divide across regions, personal data protection, cybersecurity, and most recently, digital sovereignty. We strive to find a way to translate into our canons of understanding, a world by now predominantly made of totally digitized ecosystems.

The result of the inextricable integration of an endless array of technology platforms and applications, responding to rules largely invisible to the end users, almost impossible to be verified objectively. In the hands of software developers who wield the creative power of inventing new systems, machines, and products from the ground up, this dynamic has led to an unprecedented level of stochastic uncontrollability - something that humans are increasingly unable to manage. What is needed is a new awareness of the digital world, not as a simple set of technologies, but as a true parallel ecosystem to the physical one, increasingly independent and autonomous.

It is therefore necessary to create new paradigms of governance, which will accelerate the exit from the era of fear and 'control' of technology, and the transition to a new era of trust and 'economic evolution' through technology.

10.2 Digital sovereignty or digital autonomy?

They sound synonymous but are not.

Sovereignty is a political concept, applicable to boundaries within which a specific jurisdiction - that is the application of specific laws - must be exercised.

Autonomy, on the other hand, is an independence, i.e., the opposite of the dependence we experience from today's substantial monopoly of a handful of non-European data platforms and solutions.

But it is necessary to understand that sovereignty and autonomy are closely related when talking about dependencies on raw materials, energy sources, or resources that can irreversibly affect our ability to govern a territory and its people according to their own defined rules.

The fear that a web giant, such as Microsoft, or Alphabet, or Amazon - companies with a market capitalization each greater than the GDP of any European member state, and a customer base larger than the population of any nation in the world - may in fact define their own rules, and decide not to abide to those of the countries hosting or using their services, is not unwarranted.

But if the hypothesis of the subjugation of Europe, through industrial espionage, targeted attacks, or even belligerent actions, appears to the most (not all) mere science fiction, it is not difficult to understand how the economic weight of these platforms becomes relevant at the negotiating tables on major decisions affecting the European economy. This influence is particularly evident as the European Commission is introducing with the new digital regulations (GDPR - General Data Protection Regulation, DSA - Digital Service Act, DMA - Digital Market Act, DGA - Data Governance Act, DA - Data Act, AIA - Artificial Intelligence Act, etc.).

10.2.1 A model of 'Trust' is needed.

Digital maturity has advanced significantly, and the most powerful outcome has been a new awareness, developed in recent post-Covid years, of the need for a new generation of data platforms, and more generally 'digital services', that can be 'trusted', i.e., that respond to a common 'trust' model.

The word 'trust' has thus begun to proliferate since the advent of European projects, such as Gaia-X, where the concept of 'Trust Framework' became central (trust framework = trust ruleset + ruleset verification) is central.

Gaia-X, a debated project with many critical issues, on which the hopes and frustrations of many European companies, both suppliers and consumers of cloud technologies, are seeking a real alternative to the substantial dependence on non-European platforms. Gaia-X deserves credit for having focused the effort, not in another attempt to create a European cloud technology stack (which in the best case would not even compare to its American siblings). Instead it has identified a lack of trust as the key roadblock for cloud adoption. Gaia-X has redefined digital sovereignty as the achievement of trust, and in the definition of concrete and technological mechanisms to verify the trustworthiness of existing digital services in terms of their transparency, controllability, and interoperability.

This new perspective is inclusive, yet it discriminates against those platforms that made of the opacity of their features, and the difficulty of migration, their strong point, creating constraint of client dependence effect (lock-in).

10.2.2 The digital democratization

Therefore, if trust is important, here is where magically the promise of Web3 (a more democratic, user-controlled Internet, not subject to individual checkpoints, where every action and decision is recorded indelibly and uncorruptible) seems to have a clearer meaning and value to the market.

In the new era of digital democratization, it is necessary to have software and hardware architectures with an increasing level of autonomy, which means controlled by a community of equals, and not subjugated to any individual interests. It is necessary to identify the actors collaborating in a relationship to uniquely isolate responsibilities. It is also necessary to make the characteristics of a digital service - whether it is a social media or a storage application of my personal data or photographs - intelligible. This transparency enables users to make informed choices, knowing how their data will be handled. It is necessary to implement these verifications in an automated manner. And finally, we need to build trust in this new digital ecosystem, which we initially thought we could control like traditional analogic ecosystems. However, it quickly became unmanageable due to the complexities of system integrations, and through the twists and turns of hundreds of European rules, often unverifiable, billions of lines of code unknown and never tested, trillions of access breaches and data exfiltration.

The adoption of a decentralized, autonomous architecture (DAO) can then enable secure and sovereign identification of participants in a digital collaboration, or transaction (through SSI - Self Sovereign Identity, DID - Decentralized Identity). It allows for the exposure and verification of the structure and credentials of a service with machine-readable descriptors (such as JASON-LD, SHACL, ODRL) and verify credentials digitally (through TA - Trusted Anchors). Additionally, it enables the tracking of results incorruptibly and immutably (through DLT - Digital Ledger technology and Blockchain) which shows us how it is possible to equip ourselves with a more transparent, secure, controllable, non-human manipulable technology.

In this way, technologies that would otherwise be ends in themselves, or often demonized because they are not understood (such as Blockchain, that for years was called speculative by misleadingly associating it to the use in cryptocurrencies), finally take on a clear and useful role within a specific purpose: realizing a network of services that are more transparent, controllable and interoperable with each other.

10.3 Regulation and innovation – can they live together? The reaction of the institutions: hyper-regulation

Europe and member state governments, aware of the risk and impact, have in fact already developed strategies and industrial policies to address the phenomenon and regain the so-called 'digital sovereignty,' or should we say: the technological autonomy needed to compete in any market. However, regulation alone is a double-edged sword. On the one hand, the restrictions imposed reduce the ability of operators to make the most of the potential of technology (leaving competitive advantage to countries with looser regulation). On the other hand, the cost of complying with the ever new and complex rules of the digital market (such as GDPR, DGA, DMA, DA, AIA, CSA, GIA...) allow only the few with great economic means to invest human and economic resources dedicated to compliance. This not only reinforces the competitive advantage to the big few, but making it almost impossible for end users to objectively verify such compliance. The paradoxical effect of hyper-regulation, which cannot be verified through clear and simple objective mechanisms, is an increase in distrust (a reduction in user trust). This, in turn, creates an even stronger barrier to digitally driven innovation within our supply chains. The net result is dichotomous: on the surface, Europe flaunts greater security thanks to its own regulatory productivity, but looking at market numbers the results are not supporting the optimism. The share of European data platform operators does not compete (EU 4%) with that of the two big giants (USA 74%, China 21%) grown, by the way, also thanks to a strong de-regulation in favour of data exploitation, and in open conflict with the European regulation (let's not forget that the CLOUD Act and the GDRP, the two data protection policies of US and EU, continue to be incompatible with each other, as well as with Chinese autocracy).

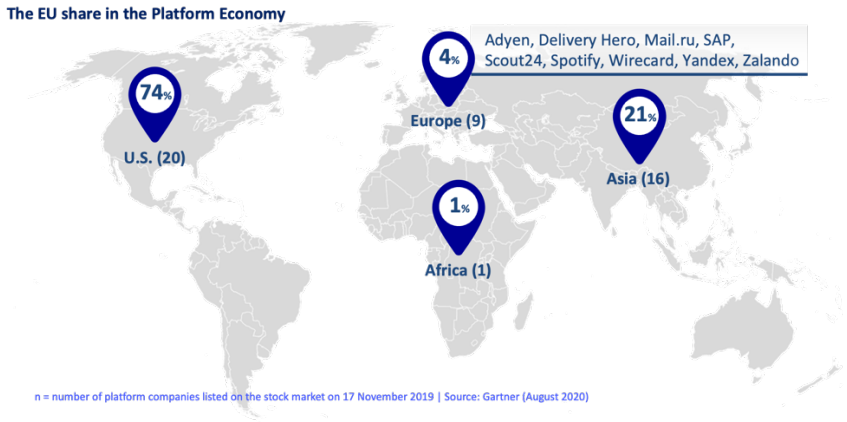

Figure 10.1 The EU share in the Platform Economy

In short, while Europe may be recognized by all as the world best referee in the digital game, we must remember that the referee never wins the match!

10.4 Ruling AI

10.4.1 Ruling AI: a regulatory asymptote

So if there is a "GDPR effect", as I call it - the risk of creating fear and mistrust in those who entrust their data to technology on the one hand, and fear of making mistakes and incurring penalties on the part of those who provide technology and services on the other, to the point of having slowed down, in many cases heavily, the migration to the cloud, the transformation of application technology parks, the reengineering of core processes and services of public administration and private enterprises. As a result, the race to innovate and create the digital economy has been hindered. What then could be the effect of a new AI Act that does not take these risks into account?

If artificial intelligence truly has endless applications, is pervasive, and it is virtually indistinguishable from any other algorithmic forms, it is in fact impossible to think of isolating it and regulating its behaviour effectively within AI powered services that are already active in thousands of platforms that we use daily.

Today we are suddenly discovering generative AI (as if we were amazed that our Golem has begun to speak) forgetting that LLM (Large Language Models) and GPT models have existed and been exploited for more than a decade, just as ML (Machine Learning) is based on mathematics from more than two centuries ago. However, what remains unseen is that AI is far more herpetic, so to speak, than we can imagine even in its most basic forms, such as RPA (Robotic Process Automation).

We remember how much RPA was demonized in the past decade because of the possible social impact caused by the reduction of jobs. Yet, during this time, the largest banks and insurance companies around the world have optimized their back office processes by automating 80% of them with RPA and adding more and more cognitive components over time (from OCR – Optical Character Recognition, to Speech2Text, to content extraction, meaning analysis, summarization, and more).

Imagine how many steps in a contract management, or customer relationship, and payment processes with an insurance, or a bank, or an ecommerce platform, already make extensive use of RPA and AI. These technologies streamline tasks that would otherwise be lengthy, burdensome, and prone to human error. Finally, let's imagine how these automata, which already replace us at work, converse with us through help desks and personal digital assistants

on our phone, which widely and deeply interact with our life sometimes without our knowledge, would automatically take decisions on financial investments (affecting our savings), purchasing at the best price a product (favoring suppliers would who know how to make themselves appealing), to determine (or discriminate) the choice of a candidate for a job position by reading thousands of CVs (that would otherwise go unread), or to propose to us in an increasingly precise and profiled way, what we need to buy, how we need to plan our leisure time, selecting our partners and friends, and so on.

Yes, all of this is troubling, yet it is already our reality - a reality where algorithms, in effect, govern us. While we must certainly regain control, we can no longer live without them. Therefore, we should stop trying to document all possible cases in which technology can hurt and should instead define a simple and common way to see through technology behaviour transparently. This would empower us to make informed decisions and start harnessing technology to its fullest potential.

It seems difficult, if not utopian, to think of harnessing AI (as well as digital in general) within prohibitive rules and legal restrictions, because of the multitude of scenarios and use cases that are impossible to predict in its complexity. Even when specific issues are identified such as the AI Act's proposed ban on the use of facial recognition in public places for the purpose of personal profiling, it remains challenging to control such technologies comprehensively. You're absolutely right - none of us wants to be monitored by a "big brother". But if we are already using our faces to unlock dozens of applications that store data on hundreds of platforms scattered around the world, through a smartphone geolocated on a satellite network and local wi-fi, the situation becomes complex. By inferring metadata - legally, since it's anonymized - biometric characteristics, location, age, race, residence, occupation, social status, shopping preferences, web interests, interests in the physical surroundings by monitoring dwell times in front of establishments... Even if this doesn't involve AI and facial recognition directly, what's the real difference? Well, perhaps the difference lies in the consent we give to the use of our data, and the fact that we should have a lot more tools to understand who we are grating access to, and then make a conscious decision about what to do.

10.4.2 A new regulatory paradigm

This is where regulation and technologies need to converge and help us rebuild trust. For instance, preventing video-metric tracking at an airport, through cameras and facial recognition with AI algorithms like YOLO (You Only Look Once), might benefit individuals who want to conceal their identity, rather than most of the people willing to allow face tracking if this gives them more physical security in return.

I'm neither an anarchist nor a digital control enthusiast, but we must understand technology before regulating it. We must accept a certain amount of risk necessary to live with technology advances and innovation that can be dangerous but should not and cannot be eradicated or put under full control (like energy according to Lavoisier's famous postulate).

This should be approached with humility and starting from hard data, especially when one does not have the necessary expertise to make decisions. It's important to consider not just the risks, but also to the benefits that technologies, such as AI, can offer. These benefits include preventing accidents, improving diagnosis of diseases, reducing human fatigue, eliminating errors and injustices, retraining repetitive jobs, and increasing control and quality of our lives.

So, no need for regulation? Far from it! However, the challenge we face is addressing the real issue, akin to solving the Gordian knot of technology. The goal is to bridge the gap between desirable theoretical regulation and its practical verifiability. We need rules that are objective, measurable, and implemented through technological platforms. These regulations should avoid ambiguous legal interpretations, costly audits, and certification processes that create barriers to entry and benefit only the certifying authorities. I am convinced that the way forward today is the development of a common set of rules defining what digital trust is, and a common European platform, open to all and inclusive, for free verification of compliance with these rules. This would provide transparency to those who choose to be inspected, showcasing their level of compliance, and allow for a healthy comparison with those who choose not to.

Contrary to popular belief, trust does not equate to cybersecurity. Trust is about verifying the veracity of a service's descriptions, and the ability to control sources, destinations, usage, filtering types of data that can or cannot be processed. It involves monitoring and tracking access, ensuring compliance with approved data usage policies, verifying the compliance to the existing regulation, legally recognizing the identity of all actors in a transaction, and legally hold the provider accountable for the statements it makes through digital signatures, and more.

There is a Digital Market Act, a Digital Services Act, a Data Governance Act, a Data Act, a Cybersecurity Act (and many cybersecurity codes in member states that differ in name but not in substance). However, there is not yet a 'Digital Trust Act' that groups into a single code sub-assemblies of the rules already defined in the various regulations, and defines how their sum constitutes a sufficient level of transparency and auditability to be considered 'trusted.'

Verification of these rules can be achieved today through technologies, such as those underlying Web3 enablers, and projects such as Gaia-X with its Trust Framework.

What we need are transparency and controllability through a common set of rules, implemented on a decentralized and distributed technology platform, to

enable informed decisions about whether to use a specific digital service. The creation of new regulations will not be sufficient, as there will always be a new Chat GPT coming around the corner and showing in a few days how to literally overturn every belief and written rule we think sufficient to feel in control of this new digital world.

10.5 The relationship between cloud and European industrial policies?

10.5.1 Economics of data

The shift to a democratic web is far from hippy idealism. In fact, it's a response to a stark reality where 90 percent of the real economy is driven by intangible assets (S&P 500 index evolution data over the past 40 years); a level of enterprise adoption of infrastructure cloud (IaaS) for corporate data management below 20% (Eurostat data 2021); a significant increase in the cloud market, tripling from 2017 to 2020, in parallel with a collapse in the market-share for European players; and an extremely powerful and opaque technological offer, capable of challenging the objective verifiability of compliance with European regulations, from the GDPR (and the legal conflict with the American CLOUD Act), to the more recent Data Act (and the lack of sufficient reversibility and interoperability) and the future AI Act (and the lack of transparency on sources and destinations of data models).

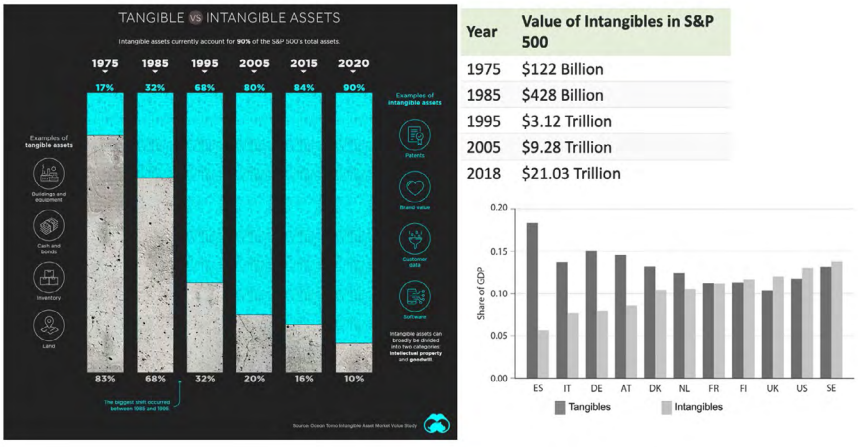

Figure 10.2 Tangible versus Intangible Assets

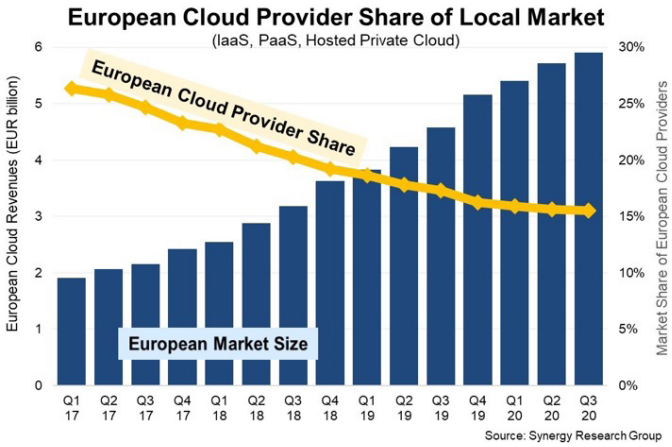

Figure 10.3 European Cloud Provider Share of Local Market

Without, therefore, a concrete alternative offering of 'trusted' services, the risk is that of a stalemate in the European real economy, and total subjugation to an oligopoly now of a very few data platform operators. The stalemate is caused by the dilemma between the fear of adopting technologies that are powerful but deemed 'insufficiently democratic,' and the fear of not keeping up with the innovation that the real economy requires, beginning to use data, pulling it out of the 'cellar' of on-premises data-centers and servers, and surrendering some of the intrinsic value to those foreign platforms managing it.

A dilemma then, in no small measure, driven by a data economy estimated in Europe by 2025 to be 830Bn Euro, about a 6% of European GDP, but which in fact represents only the tip of a submerged iceberg made up of the value induced by data to a new generation of products and services (in any sphere, from manufacturing to banking, transportation, etc.) where the market price is no longer proportional to the cost of production, but to a perceived value that is produced through the use of supply chain data (from applications to control a household appliance, to mobility services integrated into infotainment platforms, to integrations with payment systems, and so on).

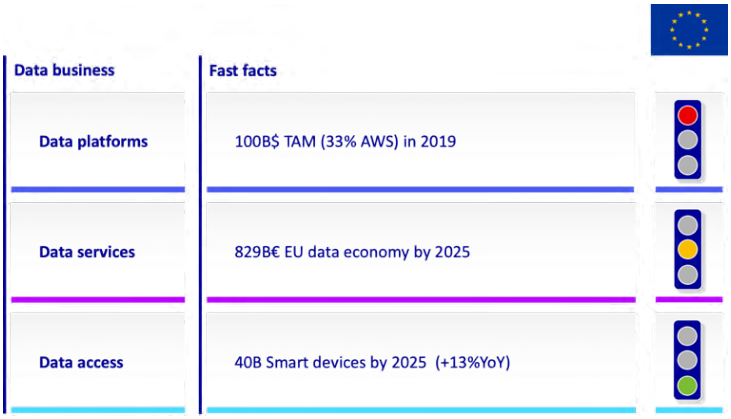

Figure 10.4 The data business

10.5.2 Data-gravity: decentralization and convergence of data platforms

Another physical phenomenon now visible to all is the so-called data-gravity, or the need to bring computing ever closer to where data is produced. This digital zero-kilometre requires a profound rethinking of cloud infrastructure. Instead of being hyper-centralized, proprietary, and isolated, cloud systems need to shift towards a federated, interoperable, and hyper-distributed model. This paradigm shift, results in the need for a continuum from cloud to Edge, and the consequent expectation to minimize data transfer, thus from data2compute to compute2data. Connectivity, in turn, becomes a hybrid of physical and virtual connection technologies, and a federation between networks and operators so that data can be accessed wherever it is generated or stored.

Yes of course, the digital divide, bringing optical fiber everywhere, creating 5G antennas, and 6G, is crucial, but the effort must be contextualized in a future that requires a geographic hyper-distribution of compute, storage, and connectivity nodes. This requires a strong federation (and therefore trust) between distributed, potentially competing operators, and a convergence between compute, storage, and network resources. These elements must be developed in tandem to prevent disconnected progress in each area. After all, we wouldn't build highways where no cars travel or sell cars where there are no roads.

10.5.2 Data-Spaces – digitalization of value chains

Like every trend, today we live a moment of strong emphasis on the importance of data. But what to do with them, and why they are so important is still largely a mystery for the many.

Everybody accepted that data is the new gold, but likewise, gold cannot feed people, build houses, or power industries - its value is intangible, just like data.

But the real difference is that the data economy built with data produces tangible effects that are visible by all and will revolutionize the world we live in.

The last wave on this data hype, which began around 2016 and consolidated recently also through the European Data Strategy, the Europe 2030 Digital Decade plan, and the investments of the European Commissions, is the creation of common dataspaces.

But what are dataspaces? Despite the many, often confusing definitions, including those who use it as a synonym of data-pools, data-lake, or data-ocean, or else.

Dataspaces are simply a virtual common space around which individual subjects (typically business actors in a value chain of any type) decide to aggregate, or federate, and share data one another for their common good.

How this is accomplished is a technical issue, but understanding why they are valuable is a fundamental economic topic. If data is the new gold, the value of data, like for gold, is intangible. Gold in fact does not feed people, generate energy, or be used to build essential goods for our life. However, gold can be converted into currency producing tangible wealth. Similarly, to monetize data they need to be converted into measurable economic benefits: a) cost reductions, b) profit increase, c) market growth. The day may come when raw or refined data will be treated directly, like utilities, materials, or enterprise shares, in stock exchange markets will come. However, for now and the foreseeable future, the value of data can be found only in specific use cases where the traditional (non-digital) processes can be simplified in costs and produce higher revenues or margins.

This process requires business analysis and business re-engineering skills to redefine and invent new ways of conducting business, and cannot happen through a mere adoption of technology. The combination of business consulting skills (business subject matter experts, business owners, product owners, business analysts) together with technologist (data scientists, AI architects, cloud architects, SW architects) is required to operate any real data-driven effective business transformation.

In the context of future data-driven economy, the dataspaces are of critical importance as they essentially serve as the digital counterparts (or data-twins) of value chains. In a digitalized value chain, the interfaces between the actors are no longer products or materials but data. In this way the end-to-end (E2E) process is seamless across all the actors, making it possible to reduce or eliminate rework, mistakes, mismatches between requirements and final product. It also facilitates impossible E2E analysis, for example the calculation of the energy consumption, or the carbon produced to build a specific product or service.

Let's give an example in the day-by-day life of healthcare.

Without common dataspaces - A patient visits a physiatrist, who prescribes a specialist consultation and an echo scan. The patient then searches for the nearest

hospital and books the exam through the hospital's booking system. After taking the exam, the patient waits for the report to bring back to the physiatrist. The physiatrist identifies the need for therapy and additional tests, and requests the patient to provide all previous test reports and medical records. Since the patient had previously lived in a different city and the records are not readily accessible, they must search through their personal records to gather the necessary information. The patient then returns to the physiatrist, who prescribes further tests, and the cycle starts anew.

With a common dataspace - The patient visits the physiatrist, who determines the need for specialized tests, starting with an echo-scan. The doctor accesses the national healthcare ecosystem platform, which connects all partner facilities and shares their availability for diagnostic tests. The system retrieves the patient's medical records and identifies the nearest lab. It also notes that the patient had been treated at a hospital in a different city and prompts the doctor to confirm or update the location preference. The doctor then books the test directly through the system. The following day, the patient undergoes the echo-scan, and the report is automatically sent to the doctor. An AI engine, analyzing millions of scans, detects a potential cancerous anomaly and sends a real-time alert to the doctor. Receiving the notification on his mobile device, the doctor reviews the image and authorizes an in-person consultation with a specialist with a simple click. While the patient waits in the hospital's waiting room, they are promptly taken to the specialist, who orders additional tests to complete the triage. The patient's entire medical history is stored and analyzed in correlation with past data. The physiatrist, having a comprehensive view of the situation, contacts the patient to discuss the next steps, which are automatically prescribed through the platform.

One may might argue that the difference is just a matter of systems integration, but the real difference lies in the approach. In the traditional model, the patient runs around the healthcare ecosystem trying to join the dots of a broken chain. In contrast, the digitalized value chain, is a whole healthcare ecosystem that is interconnected thanks to a common dataspace. Here, the patient data is at the centre of it.

The digitalization of value chains through the creation of common dataspaces is not only a way to optimize and improve existing processes and products. It represents a crucial transformation to increase the resilience of physical, geographically dispersed value chains, where a single broken ring can disrupt the full chain (as evidenced by the pandemic's impact on the automotive industry in Europe).

Common dataspaces therefore produce stronger, more competitive, more efficient, and more resilient value chains, where the cost of production, or delivery of a service, is reduced or optimized, and the margins increase proportionally

to the level of seamless integration and the depth of information exchanged by the participants.

The question then comes naturally: why has this not already been accomplished? It is not a lack of technology at all (we do have data exchange technologies since decades). Rather, it stems from a substantial lack of a common definition of trust, and a common and easy way to verify that the data exchanged respect the data usage and access policies defined by the data owners. In absence of common trust rules, value chain actors will restrict the amount of data shared scared of losing competition or intellectual property, and not leveraging the power data (keep the money under the pillow).

Still the solution is only one: a new generation of trustworthy and sovereign services.

10.5.3 A new role of leadership for Europe in the future of digital economy

Whether we are talking about artificial intelligence or digital technologies in general, we must understand that we are facing discoveries now comparable to the nuclear fusion or genetic manipulation, that can transform the entire humanity - either destroying it or protecting it depending on their use.

We should therefore first encourage and incentivize a healthy, controlled but profound phase of experimentation, to understand the benefits as well as the risks, and refine later, based on the data collected and in a continuous improvement process. And we must seek for a more effective regulation, focused more on the achievement of trust (transparency and control), and less on specific prohibitions, which are de facto already regulated by other existing codes and laws.

In the final analysis, I believe Europe is at an important crossroads. On the one hand, the choice to harness technology in hyper-regulation, hoping to force a radical (and global, since technologies have no borders) change in the way digital technologies and services are developed, delivered, sold, and enjoyed. On the other, the opportunity to translate its regulatory and legislative capacity, recognized by the world, into a huge business opportunity by developing a trust platform capable of objectively measure and verify the compliance of services with its rules.

The opportunity is thus to create a marketplace of services that can truly be defined as sovereign, fostering a new and globally competitive market. This would stand in contrast to the current dominant, often opaque solutions. By doing so, Europe could position itself as the world's leading exporter of this new generation of trustworthy technologies. This approach would align with the European Union's foundational principles of an open market, human centricity, and freedom of choice, reflecting the values of true democracy.