DIGITECCS

EMPOWERING NATIONS IN A DIGITAL AGE

D-NA | THE DIGITAL NATION MODEL

A NEW DATA AND DIGITAL GOVERNANCE FRAMEWORK FOR THE 21ST CENTURY

DALIBOR VAVRUSKA

NOVEMBER 2020

THE GAME
HAS MOVED FROM
HARDWARE TO SOFTWARE.
THE REFEREE MUST MOVE AS WELL.

CLOUDS BRING RAIN. WE NEED THEM TO LIVE. YET,
UNTIL WE PERISH, WE MUST RETAIN OUR SOUL ON EARTH AND
KEEP OUR SIGHT CLEAR TO AVOID DROWNING IN ETERNAL FOG.

A CASUAL ATTITUDE DID NOT WORK IN ENVIRONMENT, IT WON'T WORK FOR
DATA. A ROBUST DATA GOVERNANCE FRAMEWORK IS A NECESSITY FOR ORDINARY
HUMANS TO SUSTAIN A MEANINGFUL DEGREE OF CONTROL OVER THEIR OWN FUTURE.

THE MAIN THING THAT SETS HUMANS AND ANIMALS APART IS OUR ABILITY TO BELIEVE IN
FICTIONAL STORIES SUCH AS RELIGION, NATIONS, MONEY AND CORPORATES (HARARI). DIGITAL
TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE CAN COMMUNICATE AND ALSO CREATE SUCH STORIES.

CONTENTS

A NEW DATA AND DIGITAL GOVERNANCE FRAMEWORK FOR THE 21ST CENTURY

PREFACE BY AUGIE K FABELA II

If Data is the new oil, Insights are the new renewable energy. However, unlike oil, there's no limit to renewable energy. The amount of data in the world is overwhelming and it's growing rapidly. In 2020, there will be 40 zettabytes of data (40 trillion gigabytes), double the amount in 2018. This year alone every person will generate 1.7 megabytes of data in just a second. Active Internet users generate about 2.5 quintillion bytes of data each day.

Data and Insights are the energy behind what I have defined as the Second Consumer Revolution of the 21st Century. The COVID-19 lockdowns turned out to be the catalyst of this Revolution, from which the world will never turn back. This Revolution will be powered by consumers – they will determine the winners and losers of the world's digital ecosystem and this Revolution.

Dalibor puts the conversation of data governance as a fundamental topic to be addressed, by outlining in this White Paper his data and digital market governance framework, called the D-NA model. As Dalibor correctly emphasizes, the answers and solutions must put society and consumer interests at the center—they should be the ultimate beneficiaries of any solution.

The digital ecosystem is comprised of many players in technology, communications, social media, search, internet, artificial intelligence, various industries, governments, and most importantly citizens and consumers. It is all these players that must come together to create a Digital Bill of Rights that I have proposed start with the preamble: "We the people of the world have an inalienable right to digital expression, privacy, ownership of our individual digital identity, and to choose what, when, where, and how we consume everything and anything in our pursuit of convenience, lifestyle, peace of mind, and freedoms".

As for elected leaders around the world, they need to see digital and data governance as a top priority. They should focus on setting big rules, frameworks such as D-NA, the Digital Bill of Rights; as opposed to over-regulation and extensively intervening on an ad-hoc and on-going basis. Protect citizens, consumers, and the free-market economy, against the cliché: "I'm from the government, I'm here to help".

Properly leading, navigating, and defining this governance journey and framework is fundamental to fully capturing the global prosperity potential of the Second Consumer Revolution of the 21st Century.

Augie K Fabela II, is the Chairman and CEO of FastForward.ai, a Silicon-Valley social-tech firm focused on Social Retail Marketing™, Author on topics of The Second Consumer Revolution™ and the Digital Bill of Rights™, and co-Founder and Chairman Emeritus of VEON, one of the world's largest mobile operators with over 200 million customers.

HUMANS AND TECHNOLOGIES

The greatest opportunities for humans have come from technologies. However, new opportunities and freedoms are not without risks and tradeoffs. Our upcoming choices about how we embrace digital technologies will have far-reaching impact on our future society.

Technologies themselves are never good or bad. However, depending on how they are used and what values societies honour, technologies can be a force for good or otherwise.

They can bring short-term pleasure, convenience at the expense of long-term damage, or long-term benefits at the expense of short-term inconvenience. They can boost human freedoms through decentralization of decisions, or they can protect us and boost efficiency through centralization. They can disrupt our inefficient activities and organizations, or they can help to preserve them. As business opportunities keep evolving, so do policy preferences of companies. This may at times lead to tensions and even pressures to change society norms.

We govern ourselves via sovereign states accountable to citizens. While building digital economies we should treat data as assets, intervene decisively but only when justified, and assure that power is matched with accountability.

We suggest a re-think of the established approach to digital infrastructure, adoption of a new approach to national licensing for selected data and digital services, and the creation of a transparent framework for free trading in digital assets and services.

KEY HIGHLIGHTS

This White Paper proposes a new digital governance framework to nation states and groups of nation states such as the European Union (states), which want to benefit from technology-driven sustainable and inclusive prosperity, while protecting core society values such as fairness, freedom, sustainability, privacy, security and health. Technologies had a profound impact on humanity throughout history. Nothing has brought more opportunities to humans. The upcoming deployments of digital, Artificial Intelligence (AI), energy and biotech innovations are unlikely to be any different. We face spectacular new freedoms and possibilities, but there will be tradeoffs. Without the right policies, disruptions and security risks may be greater than before, and significantly more painful for large segments of population. Yuval Harari, James Arbib and Tony Seba predicted that our societies, their governance, and our approach to life are set to change dramatically due to digital technologies. The recent documentary, *Social Dilemma*, suggests that this may already be playing out. We recommend human societies make all effort to understand potential scenarios before they occur, always stay firmly in control, and make choices to protect their best interests. We govern ourselves via sovereign states accountable to citizens. Such states must meet their responsibility, implement and endorse robust data governance frameworks that facilitate efficient functioning of digital markets and AI, while protecting public interests and societal values.

To achieve such goals, we recommend policymakers to establish the concept of regulated (licensed) data and data sovereignty in carefully selected areas. Transparent governance frameworks for data, digital markets and AI require a robust definition of when data becomes a private asset, how it is harvested, transmitted, traded, protected and disposed. Private entities and communities without clear governance and accountability should not be able to use powers derived from data concentration and AI to undermine states' ability to legislate, protect citizens, protect societal values, protect free markets, and legitimately intervene in markets and societies. Regulation (licensing) for carefully selected types of data may become the key tool for allowing our established societal governance frameworks to continue functioning. We face fundamental political choices about the scope of regulatory intervention and the level of data sovereignty of individual states, their entities, other communities, and various types of AI systems.

This White Paper proposes to introduce a new national digital governance framework, the D-NA (Digital Nation) Model, which endorses separation of network infrastructure from services, alongside separation of heavily regulated data/services from lightly regulated ones, creating three independent layers:

1

INFRASTRUCTURE

2

LICENSED DATA, CLOUD AND DIGITAL SERVICES

3

OPEN MARKET DATA, CLOUD AND DIGITAL SERVICES

Ideally, D-NA will be implemented through adoption of new policies and supportive moves by the private sector. Due to synergies between licensed smart networks, licensed data and digital services, we believe that progressive, customer-centric, ideally asset light and hence flexible telecoms may be well positioned to play a constructive role in the adoption of D-NA.

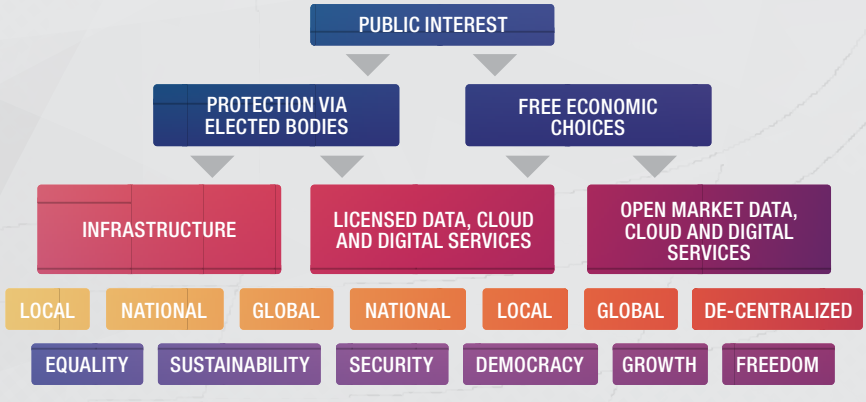
Adoption of D-NA will have a range of benefits for individuals, states, societies and humanity. It will promote economic growth by allowing investment to be frontloaded, bridge the digital divide, save resources including FX, solidify tax revenue, boost efficiency of spectrum use and boost safety, transparency and access to capital across all digital industries. Better organization of digital markets should unlock new opportunities for local and global entities to further benefit from digital platforms, big data, cloud, AI, IoT, ICT etc. D-NA will also help states and societies to tackle technological progress by creating future-proof regulatory frameworks and finding the right balance between freedoms and interests of various local and global stakeholders, and other public interests. D-NA will boost accountability of those empowered by data. It will promote societal values such as fairness, security, freedom and human centricity by adjusting governance mechanisms to better fit the digital age. Finally, it will promote sustainability and health by encouraging energy efficient and health-centered solutions while steering consumption towards more sustainable areas.

We recommend policymakers work with the key stakeholders towards implementing D-NA; establishing separate regulatory authorities for infrastructures and data; endorsing the wholesale model in national digital infrastructures with emphasis on efficiency benefits of infrastructure sharing; expanding the existing licensing for spectrum and communications to overlap with newly established licensing for specific regulated data and digital services; and building a transparent framework to promote free trading and competitive markets in data and digital assets.

Note: Option with de-emphasized competition in national infrastructure, although competition in global infrastructure may be retained (not specifically shown in the graph).

FIGURE. 1

PUBLIC CONTROL IN THE DIGITAL WORLD UNDER D-NA



Source: Digiteccs Associates

EXECUTIVE SUMMARY

Technological progress has had a profound impact on humanity. Nothing else has repeatedly brought so many new opportunities to humans. Mass market adoption of printed books, cars, plastics, vaccination, antibiotics, consumer electronics and mobile phones, for example, all showed similar patterns. Prices fell sharply as adoption scaled up, giving consumers more resources for a better life. Technologies give us spectacular new freedoms. Yet they bring major tradeoffs, including sacrifices of some liberties, as well as new security, health, environmental and wealth division challenges. Such shortcomings are often addressed via policies or better technologies. However, some long-term adverse effects are harder to detect, understand and deal with.

The upcoming technological cycle is likely to bring benefits and disruption to human societies on a so far unseen scale. Commercial breakthroughs in digital, AI, energy and bio technologies are set to follow similar patterns that we have seen in the previous technology cycles, amplified by convergence between these technologies. Global scale economies in digital technologies and AI will allow so far unprecedented centralization of data and decision-making, affecting everything from human psychology up to labour markets. In the longer-term, the following four factors are likely to have the most disruptive impact, also because they will raise fundamental questions about human rights and responsibilities:

- ability of AI to influence, if not practically control, the human mind
- use of AI to replace human decision-making on the grounds of its superiority
- ability of remotely controlled robots to operate in real-world settings
- creation of hybrids between humans and cloud connected devices

> ‘REMEMBER, GOVERNANCE IS A BIG WORD THAT INCLUDES HUMAN RIGHTS, FREEDOM OF SPEECH, ECONOMIC TRANSACTIONS ON A WORLDWIDE BASIS - IT TOUCHES EVERYTHING. IT’S EVERYWHERE, AND THAT’S WHY INTERNET GOVERNANCE IS TOPIC ‘A’ IN MANY CORNERS.’
> VINT CERF

> ‘IF YOU WANT TO MAKE A COUNTRY A COLONY, DON’T SEND TANKS IN. JUST GET THE DATA OUT.’
> YUVAL HARARI

While some of these developments are still far in the future, technology-driven disruptions are already playing out. The last century's technologies have already disrupted many natural processes in our environment, societies and even in our own bodies, putting the sustainability and social agendas to the forefront. Contemporary authors such as Yuval Harari, James Arbib and Tony Seba predict further profound changes in governance and societies on the back of digital technologies. The recent documentary, *Social Dilemma*, shows that such changes may already be playing out. Digital technologies, for example, appear to be contributing to the polarization of societies, de-stabilization of politics, and decline of public trust in the established institutions and media.

Our conscious choices about how we utilize technologies, and how we design policies governing them, will determine the future of humanity. This White Paper takes a view that our societies should make every effort to deeply understand possible long-term scenarios, stay firmly in control and make conscious choices to establish the best possible digital governance framework in the interest of humanity. Today, we govern ourselves via sovereign nation states and unions of states such as the European Union (states). Human-centricity and accountability are key attributes of such governance. Similar governance also applies to corporates and other organizations accountable to their stakeholders. Policies are generally formed and enforced by humans, who work on behalf of the public or stakeholders. However, this setup cannot be taken for granted. Our future depends on our conscious choices of which technologies we develop, deploy, constrain and potentially suppress, how we control them, whom and what we connect, how we choose to balance power with accountability, which society values we protect, and which ones we knowingly forego. Possible scenarios include the following:

- states will pro-actively oversee the adoption of crucial new technologies; they will support personal, economic and innovative freedoms while assuring that any entities empowered by data and AI are accountable through transparent governance frameworks; they will decisively intervene in carefully selected areas to protect humans, their ways of governance, their societal values and environment
- the uncontrolled global spread of technologies and data-driven AI systems will lead to divergence between power and accountability, major disruptive changes to the economic and political order, profoundly impacting national sovereignty and other core society values
- a combination of the two, possibly leading to conflicts

A number of global initiatives aimed at redesigning digital governance, reshaping digital markets and establishing AI governance are already under way in different stages. Governance and regulation of AI currently constitute one of the leading policy topics around the world. Meanwhile, de-centralized technologies such as blockchain are already offering innovative options for security, in finance, and in many other fields. Initiatives aimed at de-centralizing data and software also include Solid, backed by the founder of the internet, Sir Tim Berners-Lee; Blockstack, Dfinity etc. De-centralized technologies face issues around accountability, but they may also point to innovative governance solutions. Meanwhile, the US has been supporting global initiatives such as OpenRAN to commoditize network technologies and The Clean Network to manage security. China has been promoting ideas such as the New IP and digital multilateralism aimed among others at the role of governments. Europe's Gaia X and Russia's Sovereign Internet, as well as initiatives in other countries including India, Australia and Turkey, point to the growing interest in data sovereignty. Finally, we have seen efforts by some public bodies, such as the city of Minneapolis, to legislate combining of various data into smart ecosystems (smart cities), the so-called data quilting.

This White Paper provides guidance to nation states which want to remain in control as proxies of public interest, as they are considering their options for redesigning data, digital service and AI governance. We assume that such states want to maximize technology-driven sustainable and inclusive economic prosperity, while protecting their core societal values such as fairness, freedom, privacy, security and health. In the near-term, we see the crucial priority in rebuilding economies hit by the Covid-19 measures. In the longer term, the priority will shift towards creating efficient and safe digital markets with clearly designated and regulated shared resources. This should allow benefits of innovation to spread as deeply into all segments of the economy and society as possible. States should not only want to boost their global competitiveness, but also create an environment which enhances the value of labor and value-added provided by small and medium-sized local businesses across the widest possible segments of the economy.

We suggest governments establish the concept of regulated (licensed) data and data sovereignty in carefully selected areas, also for the sake of market efficiency. Firstly, states must establish or adopt transparent frameworks for their data markets. They need to define at which point data becomes a private asset subject to ownership rights and which data transfers constitute economic transactions.

More clarity is also needed about data harvesting, transmission, trading, protection and disposal.

Secondly, states should introduce the concept of licensing and regulation for some data, with robust governance including independent oversight. Moving to future technologies such as 5G and AI will be like moving from walking to driving. While the need to regulate pedestrian traffic was modest, states require licensing for drivers, they ban cars from driving in certain lanes, force them to stop at red lights etc. This is done for safety, but it also makes transportation more efficient. Adoption of similar approaches in data could for example break certain private data silos, and create deeper and more inclusive data markets with transparent and trustworthy oversight.

The concepts of regulated (licensed) data and data sovereignty in carefully selected areas are also crucial for governments to keep fulfilling their normal function. Even though executed by humans, governance heavily relies on data. This is becoming a major trading commodity, 'the new oil', which brings two challenges. Firstly, if certain private entities or communities without clear governance and accountability develop far superior capabilities in data and AI vs. those possessed by governments, it may undermine the established political systems and liberal democracies in similar way as the uncontrolled spread of weapons would. Secondly, excessive concentration in the data markets may severely damage free market economies, a key component of liberal democracies. Most oil products trade freely, but states get involved in the oil markets for example by securing strategic oil reserves or limiting environmental damage caused by the use of oil. Data should be approached similarly. Strategically important data may need regulatory protection and independent oversight. Activities where data can cause damage may need to be constrained. Finally, private entities may appreciate an option to enjoy sovereignty type rights for some of their own data.

Licensing and regulation of carefully selected types of data may also prevent societies from disintegrating. Data will play a similar role in the digital economy as blood does in living organisms. They require networks to flow in, like the circulation system. Different stakeholders can use data in different ways, but like with human organs, these activities require coordination to enable society to function coherently, like the human body. Major uncontrolled activities in data markets could become fatal for society, like a drug overdose for a human. Such activities may come from private companies, foreign governments or communities without clear governance and accountability. Potential solutions entail imposing physical, geographical and technological constraints on harvesting, transmitting, storing, processing and use of carefully selected types of data. Beyond that, data markets may benefit from de-centralization, democratization and de-monopolization. Technology standards, platforms and networks with limited scope for innovation may benefit from opening, interoperability and potentially turning into shared resources.

The balance between full national data sovereignty, openness to entities from allied states and global openness, including openness to communities without clear governance and accountability, are political choices which should be made by nation states specifically for different types of data. Using the transportation analogy, traffic rules are relatively globally consistent, but states retain and use their final power. Driving across national borders is possible, but there may be conditions. We see similar logic as sensible in data, digital services and AI. While some data regulations may need to be imposed on practical grounds, the overall balance between relatively strict rules and strong sovereignty vs. higher degree of openness

in data and digital services to global entities (centralization) and informal communities (communitarianism), will be pivotal political decisions, which should be approached transparently and with the public interest in mind.

The level of policy intervention in digital markets and AI should also depend on the political and philosophical balance between emphasis on free will vs. determinism. A primarily emphasis on fostering free will of individuals, while acknowledging the critical role of natural factors that we cannot scientifically predict and control, would encourage stronger policy intervention to fragment data markets and protect individuals' freedoms and privacy. This is consistent with Yuval Harari's view that advancement of digital technologies risks undermining human free will as such. Meanwhile, a policy focus on overriding societal objectives based on science-driven deterministic planning may justify a softer approach towards data-driven power concentration. This White Paper does not take a political view about the appropriate level of determinism, liberalism, libertarianism or any other ideology. It sets a framework, which enables policymakers to adopt to any given preference.

This White Paper proposes a new national digital governance framework, the D-NA (Digital Nation) Model, which endorses the separation of network infrastructure from services, alongside the separation of heavily regulated data/services from lightly regulated ones. The key aim of D-NA is to create a robust and sustainable governance framework, which strikes the right balance between nourishing innovative free markets in data, digital services and AI on one side, and establishing powerful checks and balances to protect human societies, on the other.

- D-NA empowers **governments to fulfill their normal function** in a digital age, including overseeing efficiency of markets, overseeing security and protecting certain societal values
- D-NA allows **governments to incentivize building infrastructures and potentially other shared resources**
- D-NA encourages **governments to boost transparency and oversight over trading in data, digital assets and services**, to achieve maximum benefit from technological progress, both in the local and global context

D-NA organizes digital markets alongside three layers:

1. **Infrastructure** is mostly separated from services and provided preferably on a wholesale basis; new business models are also possible ranging from lightly regulated proprietary local private networks, special purpose public networks and satellite solutions up to more heavily regulated open access nationwide public network infrastructures

2. Licensed data, cloud and digital services are data and digital services, including cloud services, deemed as crucial for the functioning of states, economies and societies or data of private entities voluntarily included into this category for their own protection; the former may include for example data/cloud services relevant for public safety and security; management of personal identities and transaction-related data (consumer credentials); transmission, processing and management of data owned by governments and selected systemically important industries; legal data interception; but also basic data connectivity (fixed-line, mobile or satellite data access), subleasing and slicing of spectrum – this White Paper is not making specific proposals about which data and services should or should not be licensed and regulated, it is only introducing this as a general concept
3. Open market data, cloud and digital services include lightly regulated software apps, platforms, big data, AI, cloud and edge computing solutions, as well as IoT and ICT solutions, all offered under a variety of business models

Ideally D-NA will be implemented through the adoption of new policies and supportive moves by the private sector; local telecoms may play a constructive role. Due to synergies between licensed smart networks, licensed data and digital services, we believe that progressive, customer-centric, ideally asset light and hence flexible telecoms are well positioned to play a constructive role in the adoption of D-NA. Under independent governance supervision they could for example carry, manage and protect regulated data, and empower other stakeholders with legitimate grounds to work with such data. This can effectively create a shield between local stakeholders and global data companies, protecting local stakeholders' security and limiting the global companies' power over certain assets. Such a shield would be used either voluntarily or on national security grounds.

Adoption of D-NA will have a range of benefits for individuals, states, societies and humanity.

1. It will promote economic growth by making it easier to frontload infrastructure investments including 5G and bridge the digital divide; save financial and FX resources by reducing infrastructure duplication; solidify transparent and fair generation of tax revenue from infrastructure and services; boost efficiency of spectrum use; boost access to capital across digital industries; create safer, more transparent and more inclusive data and digital service markets and offerings to the benefit of local economies, but also local and global players in digital platforms, big data, cloud, AI, IoT, ICT; local small and medium-sized businesses would particularly benefit from new safe and trustful digital service options under D-NA.
2. It will help states and societies tackle technological progress by creating a future-proof regulatory framework with tools to balance flexibility for innovative competition with legitimate policy interventions; empower governments to establish the right balance between local and global influence in digital economy; and allow governments to retain sufficient power to fulfill their duties including protection of state sovereignty.
3. It will promote societal values such as fairness, security, freedom and human centricity by boosting accountability of entities empowered by data (see Fig. 3); identify tradeoffs and devise robust responses to them; tackle potential excessive market power in data that could result in discrimination; give governments better tools to oversee potentially risky technologies through infrastructure consolidation and selected data licensing; give individuals more choices in privacy and security; give governments tools to defend human interests amid overlaps between the virtual and real worlds.
4. It will also promote sustainability and health by reducing energy consumption and mobile radiation from unnecessarily overlapping networks; boost environmental efficiency of our production and services; steer consumption towards more sustainable digital choices; and in some areas potentially also encourage consolidation and efficient power use in data processing and storage.

We recommend policymakers of individual states consider the following reforms:

a. Adoption of D-NA. Consider working with stakeholders to adopt D-NA. This includes making crucial political choices, driven by security and other considerations, about the scope of regulatory intervention in digital infrastructure and data, and about the level of data sovereignty for individual states.

b. Regulatory authorities. Consider establishing separate regulatory authorities for strategic infrastructures on one side, and for data together with digital services, on the other side. Strong governance in data, which should include independent elements, is particularly important.

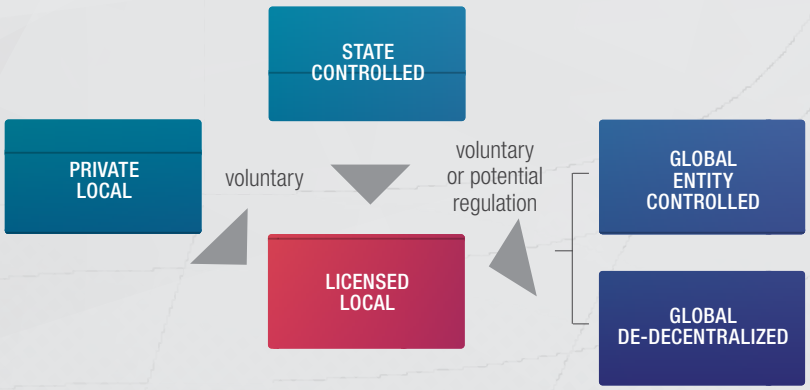
c. Infrastructure. Consider endorsing the concepts of wholesale, sharing and consolidation, but possibly also open access and structural separation, in nationwide telecom infrastructures. Acknowledge the potential emergence of new infrastructure models such as local private networks, special purpose public networks (e.g. for IoT) or satellite solutions. In areas where infrastructure competition no longer fits its purpose and monopoly solutions become practical for the states and beneficial for the stakeholders involved, consider recognizing infrastructure monopolies. Such a fundamental move would however need to be executed after careful consideration, because it would entail new regulations, most likely based on the Return on Asset Base (RAB) model, as well as regulatory suppression of competition in some areas. Similar to energy utilities, regulators would gain more say about investments and investors would enjoy predictability of returns. The market may evolve towards such an outcome gradually, over a period of time.

d. Licensed data, cloud and digital services. Consider expanding the existing licensing for spectrum, voice and data communications, to overlap with newly established licensing for specific regulated data, cloud and digital services. As discussed above, examples may potentially include data/cloud and digital services in public safety and security; consumer credentials; data belonging to governments and systemically important industries; private data requiring licensed protection; legal data interception. Additionally, licence holders may offer for example subleasing or slicing of spectrum. The new licensing of data and digital services should not always mean tightening of regulation. In areas where data is currently highly restricted, for example in medicine and biometric identification, this may in fact mean regulatory relaxation and expansion of business opportunities beyond isolated industry silos.

e. **Open market data, cloud and digital services.** Consider establishing a framework that defines at which point data becomes a private asset subject to ownership rights, which data transfers constitute economic transactions, and how to approach data harvesting, protection and disposal. Consider giving clear guidance about which data will not be subject to licensing regulations discussed in the above point, and hence free for relatively unrestricted trading. Create a framework under which all stakeholders with a lawful interest to work with regulated data will be able to do so as smoothly as possible, for example via licensed entities. Find ways to address excessive market power in data and digital services, if this is an issue. This may include for example providing fiscal incentives to smaller players such as local companies.

FIGURE. 2

SHIFT OF CONTROL AND ACCOUNTABILITY FOR SOME DATA AND DIGITAL SERVICES UNDER D-NA



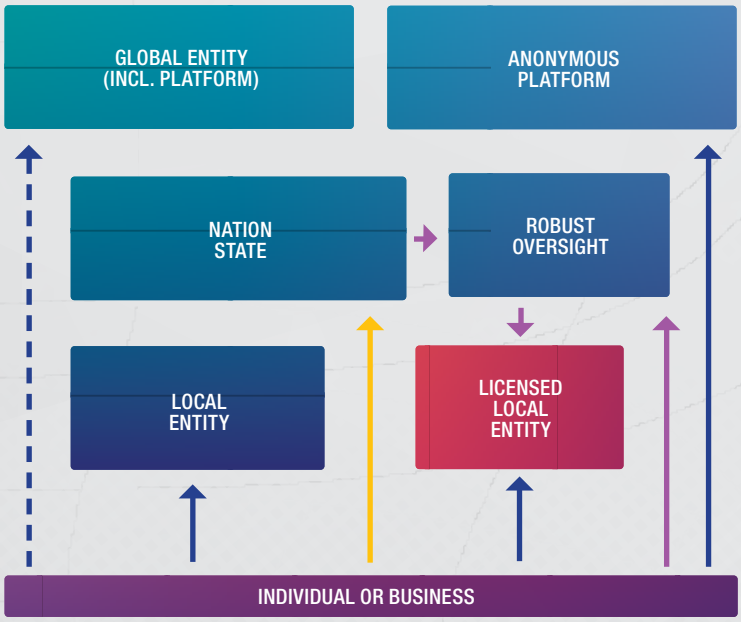
Source: Digiteccs Associates

FIGURE. 3

ACCOUNTABILITY RATIONALE FOR LOCAL LICENSING OF SOME DATA AND DIGITAL SERVICES UNDER D-NA

consumer choice
transparent supervision
democratic choice

Note (1): Democratic choice applies only to eligible voters; (2) Licensed local entity is a new concept introduced in this report as part of D-NA.



Source: Digiteccs Associates

1. THE D-NA MODEL

1.1 ESSENCE AND RATIONALE FOR THE D-NA MODEL

The D-NA model is an innovative and transformative national digital governance framework, offering principles for redesigning digital infrastructure, data, cloud, digital service, digital asset and AI markets. Its essence is in structuring all digital businesses into three independent layers:

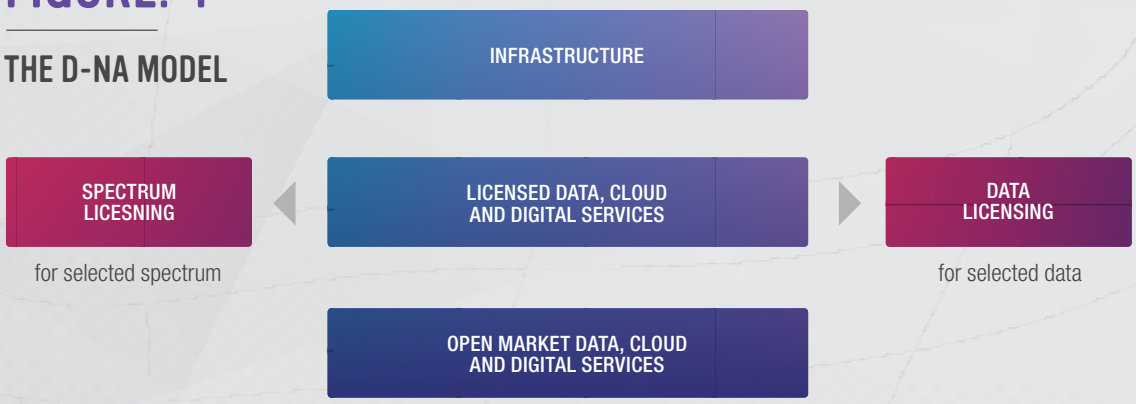
(1) **The infrastructure layer,** which includes mainly but not exclusively nationwide physical digital networks, offering access preferably on a wholesale basis.

(2) **The licensed data, cloud and digital service layer,** which includes connectivity, spectrum sharing and subleasing, data, cloud and digital services, which are deemed as crucial for functioning of states, economies and societies, or which require licensing regulation for other reasons; private entities may also voluntarily use such services for their own protection.

(3) **The open market data, cloud and digital service layer,** which includes the widest possible range of data and digital services, including cloud services, suitable for free market competition.

FIGURE. 4

THE D-NA MODEL



Source: Digiteccs Associates

While D-NA is aiming at digitally driven prosperity, it is implemented along the following two objectives:

- finding the most efficient ways for building, funding, operating and securing physical **digital infrastructures**
- finding the most efficient ways for handling **sensitive, valuable and influence-enhancing data** for the benefit of private entities and societies without excessive regulatory restriction in digital markets

FIGURE. 5

KEY IMPLEMENTATION AREAS FOR D-NA

Source: Digiteccs Associates

D-NA SERVES ECONOMIES WHILE PROTECTING ACCOUNTABILITY, PUBLIC CONTROL AND SOCIETAL VALUES IN THE DIGITAL WORLD

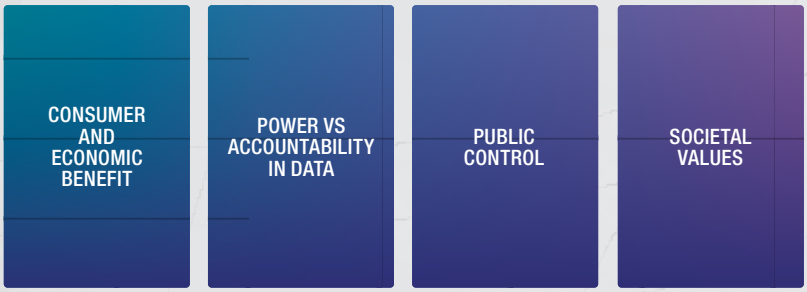
The key goals of D-NA are:

- assuring that **consumers and economies benefit** from digital opportunities and the new choices they bring
- assuring that newly created **power arising from data, digital services and AI corresponds with accountability** at all levels, with individuals and entities able to make free choices and having their fair say in rulemaking
- assuring that the **public remains ultimately in control** via its free commercial choices and elected governments, i.e. sustained national sovereignty
- protecting **societal values** including environmental sustainability, human rights, fairness, freedoms, privacy, security and health during and post the digital transformation process

FIGURE. 6

KEY GOALS OF D-NA

Source: Digiteccs Associates



1.2 HOW DOES D-NA WORK?

Each of the three layers contains different businesses with different business models. Vertical integration across different layers is strongly discouraged. For practical reasons, governments may set conditions under which overlaps are permissible, for example for overlapping ownership with separated legal entities, management and control. Below we discuss how D-NA will work in practice.

BUSINESS MODELS

In infrastructure we mainly envisage the following business models:

- Public nationwide wholesale networks, e.g. towers, fibre, Radio Access Networks (RAN). These are likely to be owned and operated by private entities. Infrastructure sharing and consolidation will be generally encouraged, particularly in areas where this is economically desirable. That said, such networks should preferably operate on a wholesale and non-discriminatory basis, while providing certain depth of population and territorial coverage. This can be achieved via a range of voluntary and regulatory measures.
- Public monopoly open access nationwide networks. It is possible that network consolidation for some infrastructures reaches a stage when competition no longer fits its purpose, and creation of nationwide monopolies becomes beneficial for the stakeholders involved. Creation of such nationwide monopolies is however a fundamental policy move, which has key implications such as new regulations, most likely implementation of the Return on Asset Based (RAB) regulatory model also used in utilities, and regulatory suppression of competition in some areas. This has to be done after very careful strategic consideration, which also takes into account alternative competing technologies such as satellite.

- Special purpose private or public networks. These are wireline or wireless networks (e.g. local Ethernet, WiFi, private 5G), often limited to the territory occupied by their owners, with different use cases and user bases. Such networks may serve one specific purpose, for example in industrial automation, or provide connectivity, for example for IoT devices or personal devices at airports, hotels etc.
- Satellite networks can complement terrestrial infrastructures.
- Region-focused competitive public networks should preferably be wholesale-based. Regulators may restrict opportunities to build and operate such networks in direct competition against nationwide networks for two reasons. Firstly, specific nationwide security and quality requirements for utility type infrastructures may apply to such networks. Secondly, when nationwide network companies voluntarily agree to invest into economically less attractive areas, they may expect certain advantages in the more attractive areas. In an extreme case, existence of RAB-based monopolies would rule out existence of competing networks.

In licensed data, cloud and digital services we envisage a small number of competing nationwide license holders focused on both retail and wholesale. Data licensing may be combined with spectrum licensing.

For open-market data, cloud and digital services we envisage a diverse set of business models ranging from subscription-based (such as Netflix), paid by personal data (e.g. Google), transaction-based (e.g. payment services), usage-based (e.g. individual movie purchases), publicly sponsored (e.g. free education and health apps), linked to a specific service (e.g. Uber or local shop apps) etc.

D-NA SHARPENS THE FOCUS OF DIFFERENT COMPANIES IN THE DIGITAL SPACE

SERVICES

The mainstream public infrastructure providers will mainly offer wholesale access to their towers, fibre, RAN networks etc. Such access should be as fair and non-discriminatory as possible. When prioritization becomes necessary, e.g. in emergencies, it will be subject to pre-established policies or commercial agreements. Private and special purpose networks may coexist with the mainstream networks, serving specific needs of private businesses and other customers.

The licensed data, cloud and digital services will initially consist of legacy services such as voice, messaging and data connectivity, consumer billing and assistance.

D-NA ENCOURAGES WHOLESALE INFRASTRUCTURE WHILE ESTABLISHING THE CONCEPT OF LICENSED AND OPEN MARKET DATA

This can be later expanded to transmitting, storing and processing of licensed data, capacity prioritization, cybersecurity services, public safety and security services, legal interception, secure IoT services, network slicing and spectrum sub-leasing. It would also include what is today called cloud services, for licensed data.

The open market data, cloud and digital services will include various consumer applications and platforms, AI, cloud and edge data services (beyond the regulated ones), ICT and IoT services.

ASSETS

The key assets in infrastructure will entail passive infrastructures (ducts, pols, towers, rooftop installations), fibre backbone and access networks, RAN and other active network equipment.

The licensed data, cloud and digital service companies will own for example spectrum licenses, selected network software and components outside what is considered as infrastructure, systems for dynamic spectrum allocation and spectrum slicing, data storage and processing capacity for cloud services, billing systems, customer relationship management systems and consumer credentials management systems. They should also be able to own and lawfully trade data and digital assets. Their ownership of infrastructure assets should be severely restricted, but for practical reasons not completely ruled out. For example, telecom operators wanting to fit into this category may be able to do so, subject to strict separation of control and management of their infrastructure units, which must provide non-discriminatory wholesale access.

OWNERSHIP OF INFRASTRUCTURE BY COMPANIES LINKED TO NON-INFRASTRUCTURE LAYERS WILL BE RESTRICTED

The open market data, cloud and digital service companies will mainly own consumer apps software and platforms, big data, ICT service businesses, data storage and processing capacity, consumer and business cloud service businesses and possibly have partnership deals with external stakeholders. Similar to the licensed national digital service companies, ownership of infrastructures by open market digital service providers will be severely restricted, but not entirely ruled out.

COMPETITION

Levels of competition in nationwide infrastructure may vary. Our default scenario is that some competition will remain in place, which may at a later stage also involve new technologies such as satellite. The role of aggressive regional public network challenges should be balanced with investment commitments of the incumbents in more challenging areas. As explained above, we would not entirely rule out the emergence of outright regulated monopolies in some infrastructures, with no national or regional challenges. Such transition would however be a fairly fundamental policy change, which should not be taken lightly. Most localized private networks will serve specific local entities; hence they are unlikely to be competing with each other.

In the licensed data, cloud and digital service market, we envisage a small number of nationwide competitors arising from the licensing process. However, the asset-light nature of these companies should assure competitive efficiency in this layer.

The open market data, cloud and digital services will ideally attract large numbers of competitors with varying business models from different industries. Excessive market power resulting from scale economies are likely to occur in some areas, which may need to be addressed via regulation. This may cause pressures to open and share resources and be subject to further scrutiny on certain platforms.

COMPETITION IS PREFERRED WHENEVER IT IS PRACTICAL, ALSO IN LICENSED DATA

REGULATION

All infrastructure will be subject to technical regulations, for example on construction planning and radiation emissions. Nationwide public networks should ideally be wholesale-focused, offering non-discriminatory access. If capacity limitations occur, any prioritization must be guided by pre-set regulatory principles, which are transparent to the market participants, or commercial agreements. Regulatory interventions in pricing may be possible in case of competition failure. If monopolies are reestablished and accepted by the regulators in some areas, a utility-like regulation RAB model may be adopted, setting investment targets and prices in such a way that implies a certain pre-set return on capital, with no additional competition accepted in a particular area. Regulators may also align rules for digital, energy, transport and other infrastructures to encourage exploitation of potential synergies. Private networks will be relatively free from regulation except on spectrum use.

D-NA LAYERS MAKE REGULATION OF DIGITAL MARKETS MORE TRANSPARENT

The licensed data, cloud and digital service providers will be subject to spectrum allocation rules, rules for spectrum use, subleasing, sharing, network slicing and obligations to provide certain services such as data connectivity to a certain quality across certain areas. Moreover, due to their involvement with licensed data, cloud and digital services, they will be subject to additional licensing conditions. Such conditions may set limits to harvesting, transmission, storing, securing processing and disposing of some licensed data, but also on trading and sharing them with other parties. For some data it may entail national data sovereignty requirements for geographical location of the stored data or obligation to provide legal data interception. Strong governance with independent supervision will be particularly important in this layer.

The open market data cloud and services will be only subject to light regulations, with the main exception of anti-trust.

CAPITAL FUNDING

Ideally, the nationwide wholesale infrastructure will be funded by long-term capital (infrastructure funds, sovereign wealth funds, pension funds), both global and local, attracted by a unique combination of relatively stable returns combined with growth. The existing telecom, energy and other infrastructure industries, along with other companies, may also take part in funding such infrastructures, although control and management separation would usually be required for telecoms. A potential decision whether to adopt the RAB based infrastructure monopoly model may also depend on access to infrastructure investors, who find such a model appealing. Local private networks are most likely to be funded by specific local businesses.

D-NA LAYERS IMPROVE THE ABILITY TO MATCH DIGITAL BUSINESSES WITH THE RIGHT TYPE OF CAPITAL

The licensed data, cloud and digital service companies will be funded by medium-long term capital, focused on growth in retail subscribers and an expanding number of services, but also growth in enterprise and wholesale services powered by expansion of the digital economy and requirements to license certain data and services. Investors in such companies will benefit from regulatory entry barriers and long-term spectrum awards. That said, local regulations will remain a crucial driver in this layer. This may attract local capital.

The open market data, cloud and digital services will be funded by growth-focused capital, suitable for the particular stage of each business (venture capital, private equity, established internet companies, public listing). The main capital attractions in this layer include market growth potential, lack of regulation and scale economies, some of which are cross-regional or global.

1.3 HOW WILL NATION STATES BENEFIT FROM D-NA?

Despite a constant flow of new technologies and innovations we have not seen any centrally coordinated fundamental reform of the internet or wireless markets since their inception 40-50 years ago. This may be because of the global nature of the internet and ecosystems around it, and subsequent lack of practical options to execute such reform. That said discussions about potential reforms have been taking place, alongside certain moves. Examples include:

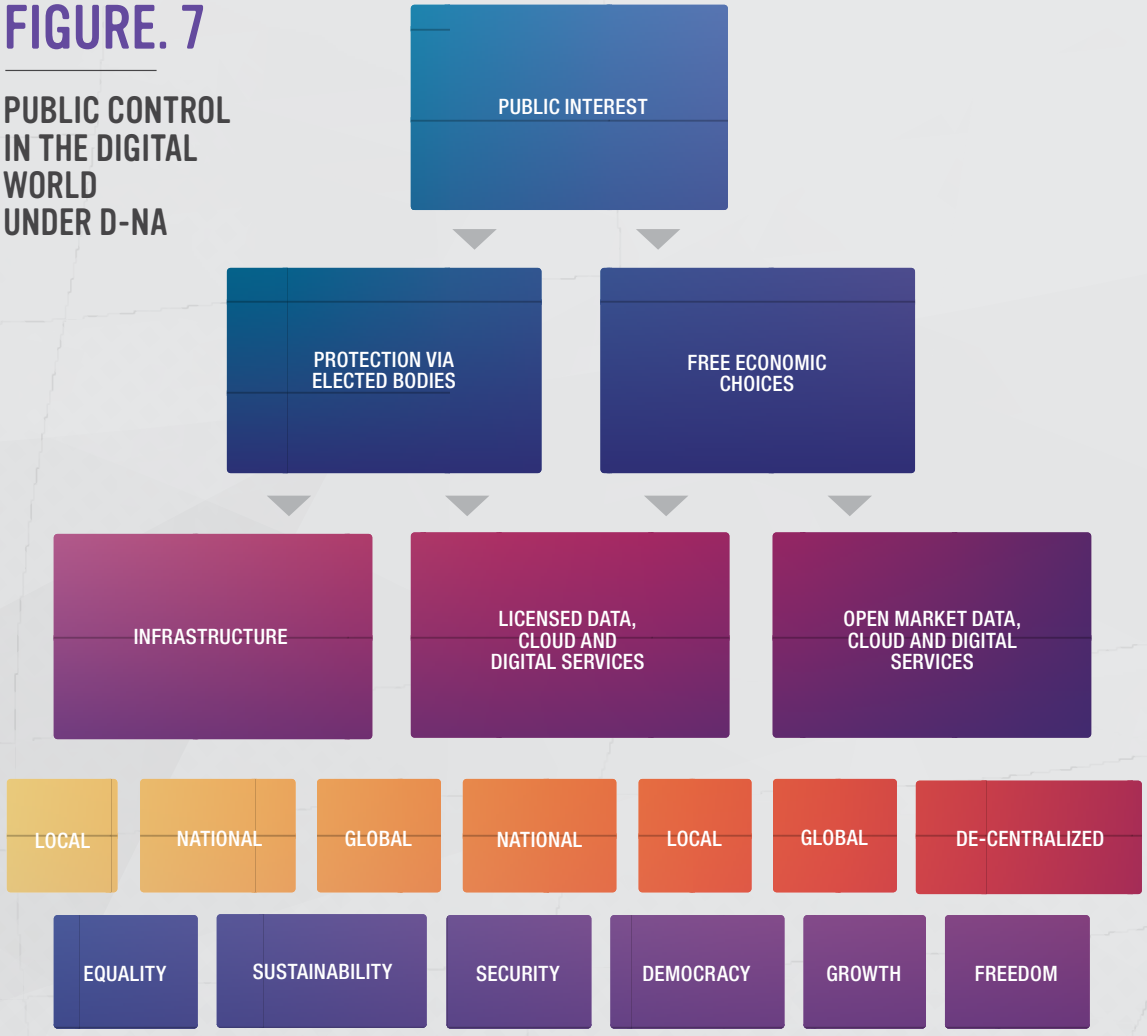
- Transition to wholesale and open access infrastructure, for example in fibre and mobile towers, in some cases leading to recreation of infrastructure monopolies.
- Efforts to regulate the IP layer via net neutrality.
- Licensing of some spectrum on a regional basis, for example for use by industrial companies or more dynamically managed spectrum licensing.
- Calls for regulation or self-regulation of dominant internet platforms.
- Efforts to regulate data privacy such as GDPR.
- Development of decentralized technologies such as blockchain.
- Efforts to virtualize network technologies such as Open RAN.
- Efforts to empower national governments, such as China-promoted the new IP and digital multilateralism.
- Efforts to certify safety of digital ecosystems such as the US Clean Network initiative.
- Efforts to boost national data sovereignty such as the Gaia X project in Europe, Sovereign Internet initiative in Russia, and other initiatives in this field in Australia, India, Turkey etc.
- Efforts to force combining some data to help projects such as smart cities, for example in the city of Minneapolis, so-called data quilting.

D-NA IS A CONCEPTUAL FRAMEWORK AIMED AT ADDRESSING THE KEY CHALLENGES OF DIGITAL TRANSFORMATION

We see D-NA as the most conceptual framework aimed at addressing the key challenges brought by digital transformation. Like in the established societies of the past century, D-NA allows the public to stay in control in the digital world through their economic choices, elected representatives and governance mechanisms (see Fig. 7). In this section we discuss how states will benefit from implementing the D-NA model.

FIGURE. 7

PUBLIC CONTROL IN THE DIGITAL WORLD UNDER D-NA



Source: Digiteccs Associates

Note: Option with de-emphasized competition in national infrastructure, although competition in global infrastructure may be retained (not specifically shown in the graph).

ECONOMIC GROWTH

The economic effects are particularly important given the need to support economic growth in the context of the impact of Covid-19.

Wholesale access, reduction of unnecessary infrastructure duplication and hence less room for arbitrage (i.e. excessive investments in some areas and lack of investment in others) will make it easier to balance the interests of nations with interests of the infrastructure industries. This will also help D-NA to **bridge the digital divide by steering some investment into rural and less economically advanced areas and 'frontload' certain digital infrastructure investments, such as fibre and 5G**, in areas where governments want to encourage economic development, including areas around transport infrastructures.

The above discussed approach to infrastructure will also **help D-NA to eliminate the cost of building and maintaining unnecessarily duplicated infrastructures, which should positively reflect on FX spending, but indirectly also on infrastructure pricing and lower need for state subsidies for infrastructure investment.** Such an approach will also make it easier to explore synergies with the existing energy and transport infrastructures, which can lead to further economic benefits.

Simplification of the infrastructure market under D-NA should also allow states **to stabilize and solidify tax revenues from their infrastructure industries.** Depending on their policy priorities, states may also have the opportunity to extract revenue from licensing of some spectrum, data, cloud and digital services. Low price elasticity in some markets may allow states to raise revenue without materially altering demand.

Making spectrum holders more asset light companies under D-NA will **boost the overall efficiency of spectrum use** through preventing the so-called 'spectrum hoarding' by owners of unique network infrastructures, and by supporting the markets for network slicing and spectrum sub leasing.

A clearer division of different digital businesses into the D-NA layers in a way that is economically sensible, but also aligned with national policies, will **improve the focus of digital companies' business models across the different layers, and hence also their access to capital and funding.**

Licensed management of consumer credentials under D-NA may help to facilitate the expansion of a safe digital consumer economy, digital commerce including microtransactions and digital ecosystems as inclusive as possible for local businesses.

D-NA BRINGS ECONOMIC BENEFITS VIA EFFICIENCY AND GROWTH STIMULATION

Better and fairer access to nationwide infrastructure on a wholesale basis as well as new opportunities to build local private networks under D-NA should maximize growth opportunities for global and local players in digital platforms, big data, cloud, AI, IoT, ICT etc.

There is an opportunity under D-NA to use new secure digital service options especially for local small and mid-sized businesses.

Any bottlenecks resulting from excessive market power in digital markets will be addressed more directly and effectively under D-NA, both in infrastructure and in data, cloud and digital services.

DEALING WITH TECHNOLOGY PROGRESS

D-NA is a future proof framework, which provides policymakers with the flexibility to choose how deeply they wish to regulate digital markets as well as tools to execute such regulation.

D-NA gives individual states a scope to balance local and global influence in digital markets, using the licensed data, cloud and digital service layer as a tool for finding the right equilibrium between the local consumer, business and national interests on one hand, and interests of the global tech companies on the other.

D-NA will also give states some powers to pursue their digital policy aims via taxation and setting licensing fees and conditions.

D-NA will encourage technological innovation by providing easier access to nationwide infrastructure as well as clarity of economic freedoms in different layers.

D-NA GIVES CONSUMERS, BUSINESSES AND STATES FUTUREPROOF CHOICES AND PROTECTION IN THE DIGITAL WORLD

D-NA enhances consumer choices around security and privacy by allowing consumers and other market players to use either open market services, or licensed services subject to special safeguards and supervision.

D-NA should permanently protect state sovereignty in the digital space, enabling governments to perform their normal function while helping to build an inclusive digital ecosystem.

D-NA better equips governments to deal with excessive market power in digital markets.

FAIRNESS, SECURITY, FREEDOM AND HUMAN CENTRICITY

D-NA aims to **match power arising from data with accountability,** which is a key prerequisite of fairness.

D-NA opens new ways to **deal with excessive market power,** which limits the scope of discrimination.

Bridging the digital divide via stronger government influence in infrastructure under D-NA will boost **economic fairness across regions and hence also employment, productivity, healthcare and education for broader segments of the population.**

D-NA allows closer **government involvement in selected areas of digital infrastructures, data, cloud and digital services to enable tighter security oversight.**

D-NA better exposes, hence addresses **tradeoffs and balances between freedom, privacy and security** in the digital world. It also gives consumers and businesses more choice in these areas.

D-NA also creates a robust regulatory framework able to **defend human interests amid the growing overlaps between the virtual and real worlds,** especially in relation to AI solutions.

GOVERNMENTS MUST STEP UP THEIR EFFORTS IN THE DIGITAL WORLD TO PROTECT SECURITY AND FREEDOM IN THE REAL WORLD

SUSTAINABILITY AND HEALTH

Reduction of unnecessary overlaps in infrastructure under D-NA will allow **savings on construction, equipment, energy and maintenance work,** with a positive impact on energy consumption and hence CO2 emissions. This approach will also reduce the number of unnecessary antennas, and hence unnecessary mobile radiation emissions.

Digital technologies promoted by D-NA will **help boost environmental efficiencies in production and services. They will also steer consumption towards environmentally-friendlier choices while providing fundamentally new options in health and well-being.**

Regulations around data security may encourage **consolidation and hence possibly better energy efficiency also in other markets such as data storage and processing.**

ENVIRONMENT AND HEALTH WILL BENEFIT FROM CONSOLIDATED INFRASTRUCTURE AND DIGITAL CONSUMER CHOICES

2. DIGITAL POLICY RECOMMENDATIONS BASED ON D-NA

2.1. THE KEY RECOMMENDATIONS

As previously described D-NA calls for separating digital markets into three distinct layers with different business models, regulations, competitive frameworks and funding options. The purist approach is full ownership and control separation, but this may be hard to establish and oversee in practice. Therefore, rules for legal, management and control separation may need to be established to define the exact requirements for D-NA.

D-NA proposes that policymakers accept the following thesis.

1. **Material parts of digital infrastructures are essentially comparable to infrastructures of national strategic utilities** such as energy.
2. **Infrastructures and data are two separate things.** Ideally they should be provided by different industries and regulated by different regulatory bodies, working alongside anti-monopoly regulators.
3. **Private data should be treated like any other private asset.** We should start by defining which data is a private asset. Free trading in private data should be encouraged when legal. Regulation should step in when there is a risk of harm. Excessive market power should be addressed.
4. **Some data is comparable to national natural resources,** meaning that it is essential for economies and security of states. It is sensible to implement special supervision of such data to assure national data sovereignty and sufficient protection.
5. **When ineffective competition persists in tech standards, networks or data,** the concept of opening should be strongly considered.

NATION STATES SHOULD SEE SOME INFRASTRUCTURES AND SOME DATA AS STRATEGIC

6. Any new powers arising from data need to be matched with **accountability.** If this cannot be efficiently achieved via free markets, elected governments need to step in.
7. **Transition to D-NA** must be executed in ways that take into account practical constraints in each country.

2.2. DIGITAL INFRASTRUCTURE

We recommend policymakers:

- establish a **regulatory body to oversee digital infrastructures;** depending on the type of infrastructures and the level of competition, such authority may have certain influence on **operations, investments, technological choices, technical specifications, security and strategic protection of such infrastructures,** alongside their alignment with other strategic infrastructures such as energy
- consider **endorsing the concepts of wholesale access, sharing, consolidation and in some cases also open access and structural separation** in nationwide telecom infrastructures
- consider endorsing the concept of **non-discriminatory access to nationwide digital infrastructures with conditions governing situations when there is shortage of capacity**
- in areas where infrastructure competition no longer fits its purpose and monopoly solutions become practical for the states, and beneficial for the involved stakeholders, **consider recognizing infrastructure monopolies;** such a fundamental move would however need to be executed after careful consideration, because it would entail new regulations, most likely based on the Return on Asset Base (RAB) model, as well as regulatory suppression of competition in some areas; similar to energy utilities, regulators would gain more say about investments and investors would enjoy predictability of returns
- if sensible, support **step-by-step evolution towards the infrastructure monopoly model**
- acknowledge the potential emergence of new infrastructure models such as local private networks, special purpose public networks (e.g. for IoT) or satellite solutions

- make **building national digital infrastructures as smooth as possible,** for example by tackling unnecessary red tape and securing support from public entities
- consider an optimal **ownership model for national digital infrastructures,** including the involvement of national wealth funds and long-term infrastructure investors
- regulate **mobile radiation limits** in national wireless infrastructures and other public and private networks, based on the best available scientific evidence at each time

2.3. LICENSED DIGITAL SERVICES

We recommend policymakers:

- consider **expanding the existing licensing for spectrum, voice and data communications (connectivity), to overlap with newly established licensing for specific regulated data, cloud and digital services;** examples for new licensing may potentially include data/cloud and digital services in public safety and security, consumer credentials, data belonging to governments and systemically important industries, private data requiring licensed protection and legal data interception
- establish a regulatory body to oversee licensed spectrum and data markets, including management of licensing for selected spectrum, data, cloud and digital services, and enforcement of the licensing conditions
- consider a framework to support network slicing, spectrum subleasing and possibly dynamic allocation of some spectrum
- replace the relatively narrow concept of net neutrality (mandatory opening of networks at the IP layer) by a broader concept of opening of tech standards, networks and platforms depending on competitive efficiency of the respective markets
- address the need for prioritization of strategically important national services (such as emergency services) in the licensing process
- assure that **licensed connectivity, data, cloud and digital services are widely provided on a wholesale basis** to all business entities, to achieve robust and inclusive local digital economies with smooth access to legally available licensed data

D-NA PROPOSES WHOLESALE NATIONAL INFRASTRUCTURES, BUT SUITABILITY OF RAB MONOPOLIES DEPENDS ON CIRCUMSTANCES

COMBINING SPECTRUM LICENSING WITH LICENSING OF SELECTED DATA, CLOUD AND DIGITAL SERVICES APPEARS SENSIBLE

- consider **selectively allowing spectrum sharing** when this brings otherwise hard-to-achieve practical benefits, however assuming that this does not materially distort competition between spectrum-holding licensed data, cloud and digital service providers
- in higher frequency bands, find the **right balance between allocating spectrum to nationwide digital service providers and other use cases,** including unlicensed or dynamically allocated spectrum for local private networks
- facilitate **fair and transparent communication with the public about how and why national governments regulate data**

2.4. OPEN MARKET DATA, CLOUD AND DIGITAL SERVICES

We recommend policymakers:

- consider **establishing a framework that defines at which point data becomes a private asset subject to ownership rights**, which data transfers constitute economic transactions, and how to approach data harvesting, protection and disposal
- consider giving clear **guidance about which data will not be subject to licensing regulations** discussed in the above point, and hence free for relatively unrestricted trading
- provide **guidance about potential privacy and security regulations that apply across all data categories and businesses** (e.g. GDPR) while trying to minimize the scope of such broad-based regulations
- find **ways to address excessive market power in data and digital services,** if this is an issue; this may include for example providing fiscal incentives to smaller players such as local companies
- support **de-centralization, democratization and de-monopolization in data and digital services** outside the scope of licensed and regulated segments

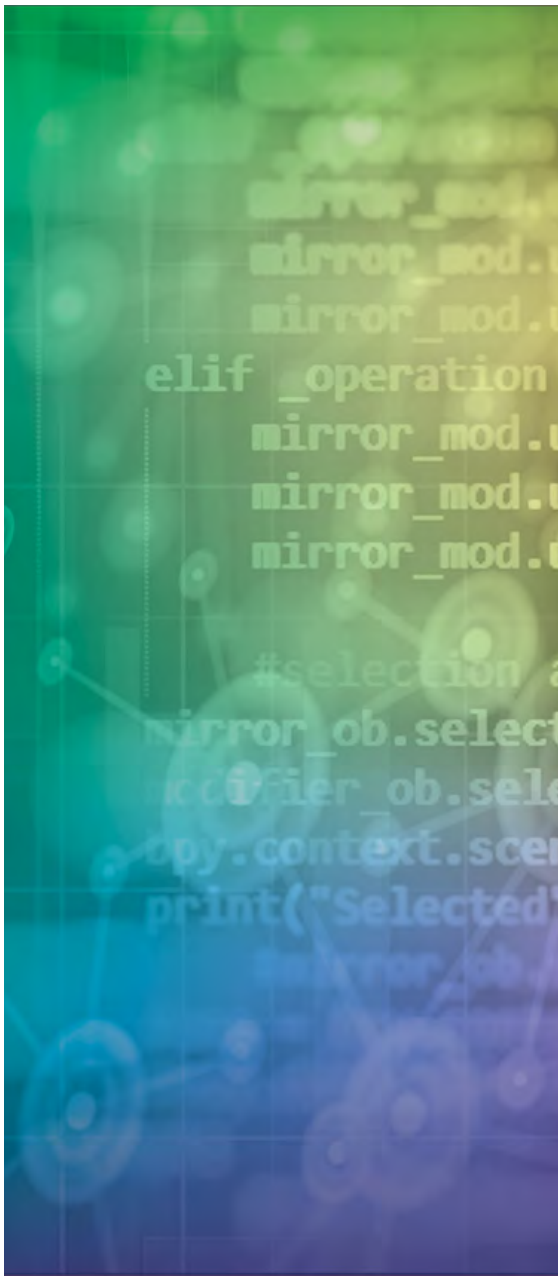
D-NA PROPOSES EITHER DE-REGULATED DATA OR SMOOTH ACCESS TO REGULATED DATA VIA LICENSED ENTITIES

3. IMPLEMENTATION AND KEY QUESTIONS ABOUT D-NA

3.1. BALANCING STAKEHOLDERS' INTERESTS THROUGH D-NA

Designing a digital economy with a blank sheet of paper would be one thing, but implementing a solution to a specific situation in a specific country in a global context is a completely different thing. Implementation of D-NA will require transformation of the local telecommunication and ICT industries and some adjustment of the role of global technology players. It is therefore unsurprising that conflicts of interests may arise involving the following parties:

- Consumers and citizens often have conflicting interests ranging from cheap, fast and reliable broadband connection, available across national territories, and a wide range of well-functioning consumer services such as social networks, e-commerce or personal cloud. New areas of interests have been emerging, such as privacy, cybersecurity, protection from harmful content, online freedoms and credible e-voting right the way through to mobile radiation security.
- The legacy telecoms usually want limited disruption to the status quo, apart from the removal of regulations that adversely affect them. They usually argue in support of infrastructure consolidation and sharing, but they rarely want outright infrastructure monopolies due to regulatory concerns. They have so far been too risk averse to push their own distinct reformist agenda in digital markets.
- Global internet tech usually wants minimal regulation in technologies and digital services, but also globally universal standards for network opening, so far especially net neutrality. Global interbit tech generally opposes concepts of national data sovereignty. It benefits from any measures that lead to expansion of infrastructure accessible for its products and services.



- Global telecom equipment vendors mainly want environments that support network investments. Security of mobile equipment has also become an issue in the past years.
- Large businesses and public institutions are usually interested in strong nationwide digital infrastructures, but also in their own ability to build protected data silos and even private networks on grounds of trust and security. They increasingly need access the most advanced cloud and AI solutions. Sometimes they may demand local spectrum. Open national infrastructures would come as a benefit for them.

- Small local businesses in all sectors have principally similar interests to large businesses. The main difference is that they can less afford investing into their own ICT systems. Hence, they are more deeply reliant on external network, data, cloud and digital services. External trustful and secure solutions will hence be important for them throughout a larger range of products and services.
- Smaller and mid-sized ICT and tech companies are usually interested in strong digital infrastructures, open access to such infrastructures and pro-digitalization policies. They also benefit from barriers preventing larger tech companies, both at a global and national level, from competing for their business, such as needs for customization, trust etc.
- Local digital infrastructure companies usually support an open access infrastructure model and limited infrastructure competition. Some of them prefer regulated local or nationwide monopolies, which give them a predictable return on investments. However, those potentially enjoying high returns may not support such regulations.
- Telecom infrastructure challengers usually want pro-competitive and ideally asymmetric regulations to disrupt the established telecoms. For example, they often want lighter or no investment obligations compared to the incumbents. Meanwhile, they want access to the incumbent networks at regulated terms. They are naturally opposed to nationwide infrastructure monopolies, although some of them may support the concept of fragmenting the market into local open access monopolies.
- Established local energy and other utilities. Some local energy and other utilities are interested in investing into digital infrastructures due to their own needs as well as synergies with their existing infrastructures.

D-NA aims to find a fair solution to address legitimate interests and the needs and concerns of all the involved stakeholders. The key for D-NA is in balancing power arising from data with accountability. Since elected governments have major responsibilities and accountability to the general public, they must get fair share of influence in the digital space as well. D-NA aims to assure that market-based mechanisms allow them to use such influence as efficiently as possible.

TO FULFIL THEIR RESPONSIBILITIES, GOVERNMENTS NEED MORE POWER IN DATA; D-NA AIMS TO ACHIEVE THIS BY ESTABLISHING A FAIR AND OPEN DATA GOVERNANCE FRAMEWORK

3.2. POTENTIAL PRACTICAL USES OF DATA LICENSING

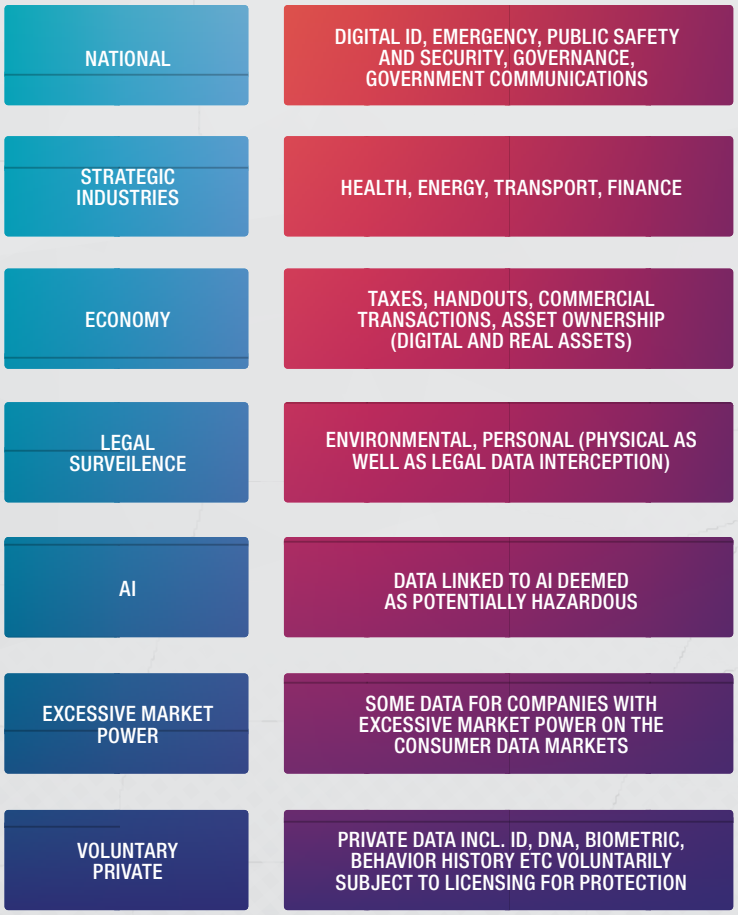
DATA LICENSING HELPS STATES, STRATEGIC INDUSTRIES AND THE BROADER ECONOMY, WHILE TACKLING SECURITY RISKS AND MONOPOLY POWER

Fig. 8 shows potential practical uses of the licensed data concepts. This White Paper does not make specific recommendations about which data should be put under a licensing regime and what type of constraints such a licensing regime should impose. However, we show types of data, for which licensing would potentially make sense on a basis of normal scope of responsibility of national governments.

We also note that even if D-NA is not adopted as part of nationwide regulation, some of the practical use cases could still be implemented via self-regulation or other forms of self-imposed governance, assuming that it convinces private entities to give more trust, for example to the telecom and local digital companies, and voluntarily mandate them to manage their data, private 5G networks etc.

FIGURE. 8

EXAMPLES OF AREAS WHERE DATA LICENSING COULD MAKE SENSE



Source: Digiteccs Associates

3.3. KEY QUESTIONS

Below we answer additional questions about D-NA.

1/ CAN GOVERNMENTS REALISTICALLY ADOPT D-NA AMID THE ALREADY GLOBALIZED TECH AND INTERNET INDUSTRIES?

The nature of the globalized market is a key regulatory challenge in data, cloud and digital services. It is hard to define national markets, over which national regulators would have jurisdiction. It is equally hard to agree coordinated global regulatory responses. Regulating international trade with data services is also hard, because of consumer expectations (of unrestricted and seemingly free access to data around the globe), international trading treaties as well as practicalities around overseeing data activities, which are often hard to track. Another challenge comes from the immense global complexity of various corporates and partnerships between them, which means that nearly any proposed policy change would harm every corporate in some sense. Reliance of consumers and national economies on global internet services does not particularly help either.

However, there is a growing consensus that some reforms in the digital space are needed ahead of the large-scale adoption of AI. If the reformist efforts are delayed, it is likely that conditions for implementing such reform may deteriorate further. There is also nothing in the D-NA concept which explicitly stops national governments from cooperating with other nation states, unions of states such as the European Union, and global organizations to improve their leverage, as long as there is transparency about what degree of national sovereignty will be maintained.

While adoption of D-NA will naturally mean risks, the previous section implies that it would also bring benefits to many stakeholders, while making our governance more sustainable. On the practical side, it may break local and industry data silos and expand data and technology solutions nationwide, bringing both scale economy and protecting data sovereignty.

Moreover, adoption of D-NA does not have to focus mainly on the existing data services. Instead, it can focus on yet to be developed data, cloud and digital services, and hence not necessarily disrupt the existing global tech business.

TECH GLOBALIZATION MAKES DIGITAL REFORMS HARD, BUT AI MAKES THEM INEVITABLE. D-NA STRIVES TO MAKE THEM PRACTICAL

2/ WILL DATA REGULATION NOT ADVERSELY AFFECT NATIONAL ECONOMIES?

There are several possible views on global data governance. One is that global consolidation in data is practically inevitable, and in fact necessary, for economic and societal progress. Nations that choose to restrict and regulate data, will be left behind economically. An alternative view is that data should be de-centralized, giving maximum power to individual users and small groups, without any respect to companies and national borders.

What is clear though is that data will attract more economic and political power. Hence the ways in which we shape up our data markets are extremely important, also for our economy.

Assuming that data is an asset, a trading commodity, there is no economic evidence to suggest that allowing it to concentrate into quasi monopolies is good for the long-term prospects of economies, especially in countries that do not host such quasi monopoly tech companies. Historical evidence also suggests that economic prosperity is usually achieved in well governed societies with clear enforcement of justice, which may be hard to achieve with excessive data concentration or de-centralized systems. As in the past, national economic prosperity will be best served by having well-functioning, diverse and well governed markets in data. Reasonable interventions alongside the D-NA principles may even achieve economic benefits by breaking local data silos, boosting interoperability of local IT systems and offering local businesses trustful solutions. Cross national cooperation and focus on new (as opposed to already established) services may be used to better align D-NA with the interests of big tech.

TOO RELAXED AN APPROACH TO DATA IS UNLIKELY TO BRING NATION STATES SUSTAINED ADVANTAGES

3/ COULD DATA REGULATION SUPPRESS DEMOCRACY AND LIBERAL ECONOMY?

It is hard to precisely define democracy, but the following applies:

a/ **Democracies are strongly linked to nation states.** The main manifestation of citizens exercising their democratic rights is via the election of their national state representatives. Anything that undermines nation states would therefore undermine democracy.

b/ **Democratic societies have checks and balances that prevent any single entity or group, global or local, from becoming the absolute arbiter of the truth, rights and wrongs.** Such checks and balances have to extend into the digital world.

c/ If not regulated, digital technologies may manipulate (hack) people themselves, and undermine their free will. As Yuval Harari pointed AI systems may learn to know individual people better than they know themselves. This opens an opportunity to offer unmatchable advice for personal decisions, and subsequently manipulate people on a previously unseen scale, effectively suppressing their free will.

d/ If not regulated, data technologies can significantly interfere with politics. Following on from the previous point, the ability of today's leading digital platforms to use their dominance on the data market to manipulate elections has been well explained, for example by Dr. Robert Epstein.

e/ If not regulated, data technologies can undermine liberal economies. According to Yuval Harari the notion that free markets always lead to the most efficient economic outcome is not universally valid. If a particular centralized AI system, for example, obtains superior information to what each of the market participants has at each time, such a system would produce economically superior decisions compared to free markets. This is a real threat to the concept of liberal economies, and one of the most fundamental points in the data and AI regulation debate.

f/ Democracies simply need new tools to deal with the unprecedented increase in collected data. Technologies allow the collection of data, the combination of which could be extremely useful as well as hazardous. This includes, for example, human DNA genome information, medical histories, biometrics, unique voice ID, online behavior history, history of physical presence, contacts and activities. Some of this data must be strongly overseen to preserve human dignity, free will and hence democracy.

D-NA aims to regulate data in ways that mitigate the above-described challenges, to promote rather than suppress democracy and liberal economy. In other words, it encourages introduction of governance checks and balances to the digital world, which would be normal in the real world. Naturally, no governance system is perfect, and risks of abuse will always exist, but this should not be the reason for not introducing such checks and balances. As humans we have created the digital world and unless we want it to uncontrollably disrupt our real world, we must govern the digital one.

TO RETAIN DEMOCRACY AND LIBERAL ECONOMY, WE MUST INTRODUCE CHECKS AND BALANCES IN THE DIGITAL WORLD, WHICH WE HAVE CREATED

THE CHANGING ROLE OF DIGITAL SERVICES MEANS THAT GOVERNMENTS WILL HAVE TO MAKE CHOICES IN AREAS WHERE THEIR INVOLVEMENT WAS UNTHINKABLE BEFORE

4/ WHY SHOULD GOVERNMENTS BE MAKING SOME TECHNOLOGY CHOICES FOR INFRASTRUCTURES AND DATA?

Historically, national governments have been heavily involved in making technology choices, for example in energy including nuclear power, defense and healthcare, but also for example in wireless networks. That said they have largely stayed away from making such choices in data technologies. With the growing importance of connectivity and data, we see the following case for involvement of national governments in technology choices;

a/ **Choices of globally standardized wireless technologies such as 5G** should be endorsed and demanded by governments.

b/ Choices of certain technologies and technology vendors may involve **security or health risks.**

c/ Choices to **'frontload' certain investments particularly in infrastructure, or to deepen network coverage,** when done in line with broader frameworks of the infrastructure markets, may play an important role in national economic policies.

d/ Choices to **secure strategically important data,** or to influence the ways in which such data is handled.

e/ **Choices to restrict certain AI technologies,** preferably through regulating data used by such technologies (e.g. face recognition) on the grounds of security or societal values.

5/ CAN DATA REGULATION TRIGGER PUBLIC OPPOSITION?

The internet has been built around the notions of freedom and equality. Therefore, any attempts to regulate or restrict popular services are likely to trigger public opposition. For example, a number of states would likely wish to restrict encrypted messaging such as WhatsApp, to allow legal interception in a fight against terrorism and crime, but not too many of them have done this. Meanwhile, consumers are increasingly attracted to the so called de-centralized digital solutions, such as cryptocurrencies, which aim to move influence over data further away not only from governments, but also corporates and other institutions.

The reality however, sometimes differs from perceptions. In the real-world, freedom and accountability go hand-in-hand. So far, we have seen mainly two models of governance for consumer data.

- Big tech has used data to accumulate significant power, which is not always matched with accountability. As a result, we have seen issues such as 'fake news', mind manipulation, possible discrimination etc., also described in the *Social Dilemma* documentary.
- De-centralized systems lack true accountability, i.e. their functioning practically depends on the religious-like faith of individual users in the system and its principles. This also applies to cryptocurrencies, the existence of which entirely depends on behaviors driven by expectations of their future value. Moreover, systems presented as de-centralized are not always entirely so, while their true governance may not always be transparent.

We see a scope to convince at least some consumers and citizens about the weaknesses of the existing data governance options, especially as consumers are increasingly interested in privacy, cybersecurity, protection against harmful content, online freedoms etc.

The Covid-19 pandemic showed the importance of nation states in protecting citizens, it has raised awareness about tradeoffs between freedoms and security. This may set grounds for the potential introduction of new governance frameworks in data. As long as they are trustworthy and fair, with well explained checks and balances, it is quite possible that the public would accept it. Once the understanding is built that data should be seen as any other asset, even legal data interception may be seen as comparable to police physically arresting criminals. It is all about the trust of the framework and system.

COVID-19 SHOWED THAT THE BUCK ULTIMATELY STOPS WITH GOVERNMENTS. IT MUST ALSO DO SO WITH DATA, DESPITE BIG TECH AND DECENTRALIZED MODELS

6/ COULD ELECTION CYCLES AND POLITICAL INSTABILITY PROVE OBSTACLES IN INTRODUCING D-NA AND DATA REGULATION?

Instability and short-term focus in politics are quite common today. The implementation of D-NA may take a relatively long time and it involves execution risks. Naturally, this does not help when dealing with large-scale cash rich global tech companies with well thought through long-term strategies, very strong knowledge and research capabilities. That said we think that the issue of data governance will only grow in its importance and nation states will understand that successfully addressing it will even become a question of their own survival. D-NA offers a framework that should hopefully be broadly agreeable for any leaders who want to sustain nation states, giving them flexibility to reflect their specific political preferences.

D-NA PROVIDES A UNIVERSAL FRAMEWORK WHICH CAN SUSTAIN POLITICAL INSTABILITY

7/ HOW SHOULD LOCAL TELECOM COMPANIES ADAPT TO D-NA? CAN THEY CONTINUE OWNING SOME INFRASTRUCTURE?

The telecoms industry would obviously be affected by the adoption of D-NA in a major way. Telecom companies currently tend to be conservative, and usually oppose major changes. That said we believe that D-NA also brings significant opportunities for telecoms to grow their value via win-win situations. This comes from two areas: consolidation of infrastructures, including better predictability of returns on infrastructure investments, together with new opportunities in licensed data.

D-NA makes a clear distinction between infrastructure and the data business, which includes big data, cloud, digital and AI services. Practically, the established telecom operators will have three choices.

D-NA SEPARATES PHYSICAL INFRASTRUCTURE FROM DIGITAL SERVICES. ANY CROSS-OWNERSHIP IS SUBJECT TO STRICT RULES

1. They can dispose of their physical infrastructures, potentially taking advantage of a consolidation process.
2. They can dispose or suppress their customer businesses and turn into wholesale infrastructure players.
3. They can internally separate their infrastructure units to establish entirely independent management and control, while pursuing opportunities in licensed data, cloud and digital services.

8/ WHY DOES D-NA PROPOSE THREE LAYERS? WOULD A TWO-LAYER INFRASTRUCTURE VS. SERVICE SEPARATION NOT BE SUFFICIENT?

Starting with tower spin offs, various forms of separating infrastructure and services have been occurring in telecoms for more than a decade. Although not all deals separate infrastructures in exactly the same ways (passive, active, sharing, legal separations, full disposals etc), most of the deals have been driven by short-term economic reasons based on a fact that standalone infrastructures tend to be worth more than infrastructures embedded in integrated companies. For this, a two-layer model is sufficient.

THE MIDDLE LAYER CREATES WIN-WIN OPPORTUNITIES FOR GOVERNMENTS, TELECOMS, BUSINESSES AND BEYOND

The fundamental reason for adding the third layer in D-NA is linked to a notion that licensing regulation of data, cloud and digital services would be helpful for nation states. In such cases, the creation of the middle layer will be a win-win solution. While governments gain a new opportunity to establish robust data governance, telecoms will get a natural new space to expand into, organically and via M&A.

9/ WHY SHOULD SPECTRUM STAY OUTSIDE THE INFRASTRUCTURE LAYER IN A LICENSED BUT COMPETITIVE LAYER?

When infrastructure becomes a shared asset, used predominantly through wholesale access, questions arise whether spectrum should not be part of such infrastructure. Combining infrastructure with spectrum would create a fully-fledged nationwide open access wireless network. Some countries including Mexico and South Africa have been contemplating such ideas with varying degrees of success. However, we believe that the reasons for keeping spectrum outside the physical infrastructure layer in a separate competitive layer remain strong.

a/ If infrastructure does not get fully monopolized and combined with all licensed spectrum, allocations of spectrum would have to be realigned with the new setup of wholesale infrastructures. Practically, this would not only be complicated, but also economically difficult, because the level of desirable competition in spectrum is likely to be higher than in some infrastructures. This problem would further escalate for monopolized infrastructures.

b/ Any fundamental changes in spectrum allocations would practically mean forced dismantling of the existing telecoms industry, which may be illegal, impractical and uneconomical.

c/ Equipping infrastructures with newly allocated spectrum while keeping the previous allocations intact would be problematic. It would fragment spectrum allocations between different business models.

d/ Competition between spectrum holders will help to boost efficiency of spectrum use and reduce the risk of spectrum hoarding.

e/ It is possible to clearly divide physical infrastructure for wireless networks from the actual ‘virtualized’ networks, which use spectrum. Hence spectrum does not need to be combined with infrastructure in one layer.

f/ Operators of small private networks may appreciate the opportunity to sublease spectrum from private entities.

COMPETITION BETWEEN SPECTRUM HOLDERS CAN BE SENSIBLE EVEN WHEN COMPETITION BETWEEN INFRASTRUCTURES LOSES ITS POINT

10/ WHY IS IT SENSIBLE TO COMBINE SPECTRUM LICENSING WITH NATIONAL DATA SERVICE LICENSING?

PROVIDERS OF LICENSED CONNECTIVITY AND DATA ARE IN A UNIQUE POSITION TO TAKE END-TO-END RESPONSIBILITY FOR STRATEGIC DIGITAL SERVICES

Holders of nationwide spectrum, mainly the telecoms at present, are also the most natural providers of basic regulated nationwide data connectivity services, both in retail and wholesale. This is why they are being licensed to use their networks to provide such services. As boundaries between software for operating data, cloud and digital services on the networks and the software for operating smart networks themselves are likely to become blurred, splitting those two areas for the purpose of licensing may bring complications.

Entities licensed to operate smart networks and handle regulated data on them will be able to take full responsibility for their work with such data in ways which were not possible in the previous ecosystems. This model will also allow the licensed data markers to be sufficiently competitive, but not too fragmented. If the existing telecom industry does not show enough expansion appetite and agility in data, there will always be options of issuing new licenses or M&A.

FURTHER NOTES

4. DIGITAL CHALLENGES FOR NATION STATES

4.1 IMPACT OF TECHNOLOGICAL INNOVATION ON ECONOMIES

The upcoming digital, AI, bio, energy and other technology innovations will have many profound effects, including the following:

- Disruption of businesses and employment. Value of human work, both in production and services, may substantially fall due to advances in automation. This will lead to employment losses in professions such as factory workers, drivers, office workers and many others. It may also lead to an abundant supply of certain previously scarce goods and services. For example, we may be able to 3D print previously expensive parts and let robots perform some household tasks. This abundance can disrupt manufacturing and service industries in similar ways that social media has already disrupted traditional media. In addition, trading can be disrupted by the ability of some market participants to obtain vastly superior information.
- New business and employment opportunities. New technologies will create highly skilled business and employment opportunities in design and implementation, although this may not be at first glance enough to outweigh disruption-driven job losses. Fortunately, the previous cycles indicate a potential silver lining. When cars, computers and travelling became cheaper and better due to technologies, the size of the respective markets grew as they appealed to larger groups of consumers. Similar effects may now happen in relation to digitalization in consumer goods, hospitality, health, well-being and other areas, which will still involve extensive human work. Finally, new more flexible ways of working may also create previously unexplored employment opportunities.

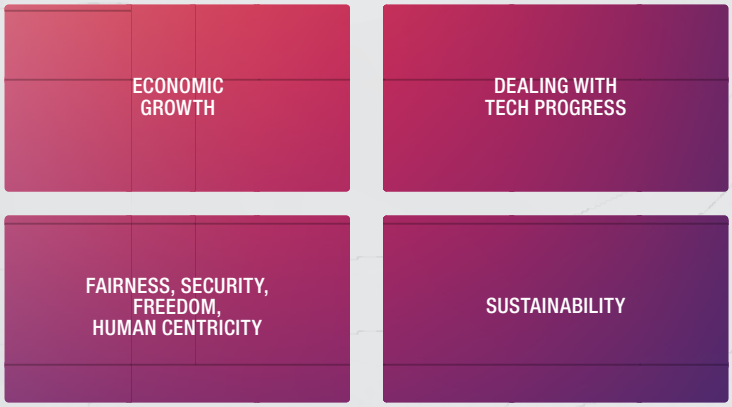
- Excessive market power. Some digital technologies have exceptionally strong scale economies, often global, and hence they are prone to cause excessive market power. If such market power gives certain entities material information advantage, which can be used in trading, this may affect the functioning of a wide range of free markets.
- Side effects. One lesson that we have learned from the current focus on sustainability is that the environmental and health side effects of technologies are not always immediately clear. The upcoming digital, AI, bio and energy technology innovations will almost certainly not be free of side effects, which will take a longer time to work out. The best thing we can do is to keep our minds open and apply sustainability concepts to all sectors and technologies from the outset.
- Ethical issues. New technologies bring new ethical dilemmas. Digital technologies will, for example, allow Orwellian-like surveillance, justified on security and health grounds, possibly used to discriminate and curb human rights. The ability to operate robots from remote locations will also change the ways we interact with the real world. Furthermore, if allowed it to do so, AI may concentrate information and render many free markets inefficient, providing better predictive and planning solutions. Ultimately, it may manipulate the human mind on a large scale, raising questions about free will. Advances in medicine and technologies linking the human brain to digital systems will also open even deeper questions about equality. All these issues ultimately have to be addressed via regulation of the respective technologies, which are ideally based on predictions and not just responses to events.

TECHNOLOGIES WILL DISRUPT AND BRING AMAZING NEW OPPORTUNITIES, BUT ALSO NEW NEEDS TO REGULATE

In summary, we see nation states having four main objectives in regard to technological innovation, see Fig. 9.

FIGURE. 9

OBJECTIVES OF NATION STATES IN REGARD TO TECHNOLOGICAL INNOVATION



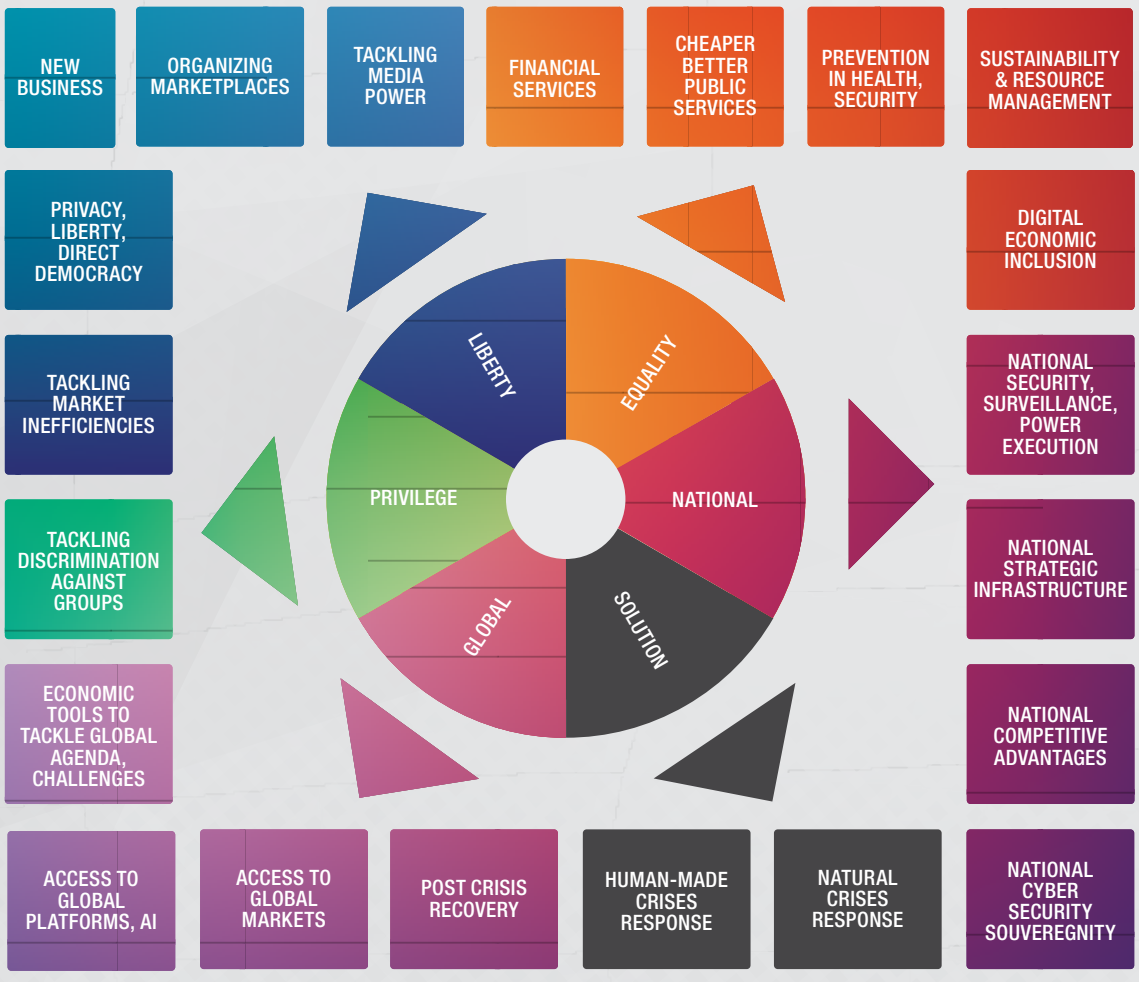
Source: Digiteccs Associates

The politics of individual nation states may evolve, and at times focus on the promotion of freedoms, liberties, equality, national interests, solving specific urgent problems, global alignment or healing past injustices. Fig. 10 shows that digital services can play a crucial role in future national governance and economies, irrespective of the underlying political priorities.

DIGITAL SERVICES WILL PLAY A CRUCIAL ROLE FOR NATION STATES IRRESPECTIVE OF THEIR POLITICAL PRIORITIES

FIGURE. 10

DIGITAL SERVICES PROVIDE SOLUTIONS IRRESPECTIVE OF POLITICAL PRIORITIES



Source: Digiteccs Associates

4.2 INEFFICIENCY IN DIGITAL MARKETS

Wireless networks and the internet gave rise to an unprecedented global market power concentration in digital technology equipment (network equipment, handsets) and digital services (digital advertising, social media etc). Local telecom operators remained positioned effectively between those two globally concentrated industries (see Fig. 11), with far less favourable scale economies and conditions for innovation. Many of them therefore mainly focused on building their own oligopolies around spectrum and networks.

However, the fact that the majority of digital innovation ended up occurring at the global level is not just a result of technologies and market forces alone. Global scale economies in data, content and internet platforms were decisively boosted also by the ideological concept of 'open internet', which separates consumer content from connectivity. This initially informal concept was later formalized as 'net neutrality' and in some countries became a law.

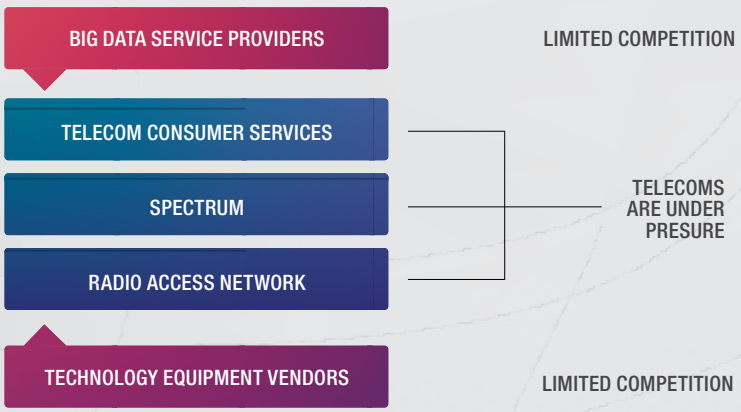
This has pushed national regulators into a challenging position. They do not have effective tools to regulate technology equipment companies or the data and content-focused tech companies in a net neutral environment. It is therefore hardly surprising that they ended up underregulating such industries, while trying to reflect their policy preferences mainly on telecoms.

As a result, the entire digital infrastructure and service markets have evolved into three distinct segments: technology, networks and data/platforms. None of the segments are particularly competitively efficient. This is in our view adversely impacting the potential of free market competition to drive innovation in the entire digital world.

DIGITAL INFRASTRUCTURE AND SERVICES HAVE EVOLVED INTO THREE SEGMENTS, NONE OF WHICH ARE COMPETITIVELY EFFICIENT

FIGURE. 11

LOCAL TELECOMS ARE POSITIONED BETWEEN TWO MARKETS WITH CONCENTRATED POWER



Source: Digiteccs Associates

4.3 LACK OF TRANSPARENCY AND EFFICIENCY IN THE BIG DATA MARKET

Data is becoming a central commodity, crucial for trading of other goods and services. Sometimes it is also called the new oil. Making sure that the data markets, including markets in processed and big data, are functioning well is therefore crucial for functioning of national economies. Preventing excessive market powers based on big data is also pivotal for ensuring the ability of open market competition to fairly distribute wealth.

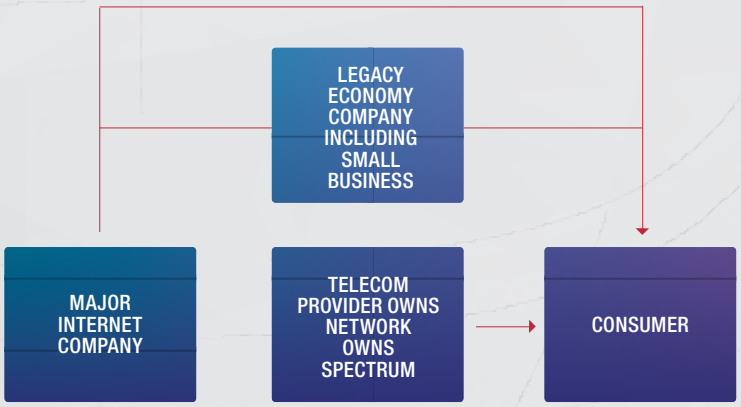
The consumer big data markets are currently dominated by large international tech companies. Fig. 12 shows that the business models of these companies are often based on using digital technologies to connect with consumers with minimum involvement of other entities from local economies. It helps these tech companies to achieve global scale efficiencies, leading to a rapid expansion of their consumer bases and hence creation of unmatched sets of consumer data. This model however raises a number of concerns:

- Consumers may be unaware or even misled about the scale of personal data they are sharing with tech companies.
- The newly created big data markets may be opaque, not very well functional, non-transparent and hard to access for independent parties, including local businesses.
- Parts of the newly created big data markets may be formally unaccounted for. When internet companies, for example, provide their customers with seemingly 'free services' in exchange for their personal data, this can be seen as a barter trade. However, normally such trades are not declared and the value of the provided service and collected data is not assessed.
- Two-tiered economies may emerge, in which local players are subject to local laws, Meanwhile, large internet platforms are not only out-of-reach for many local regulations, but they are often able to use market power to impose their own rules on local economies.
- Nation states may potentially lose data sovereignty and face cyber risks, as crucial data is stored and processed outside their borders and control.
- Big data can be abused to influence public opinion, for example via social media. This poses a threat for national governance and democracy.

IT IS HARD TO IMAGINE TRULY EFFICIENT DIGITAL ECONOMIES WITHOUT EFFICIENT BIG DATA MARKETS

FIGURE. 12

BIG INTERNET COMPANIES OFTEN BYPASS LOCAL ECONOMIES TO MAXIMIZE THEIR EFFICIENCY



Source: Digiteccs Associates

PRACTICALLY, WITHOUT A POLICY OVERHAUL, NATIONAL STATES MUST ACCEPT DIGITAL SERVICES ON TERMS OFFERED BY GLOBAL TECH

4.4 OBSTACLES TO EFFECTIVE POLICYMAKING IN DIGITAL

Given the scale of change that digital technologies are bringing, it is hard to think about successfully regulating digital markets without a significant policy overhaul. Fig. 13 shows, for example, why it is currently difficult to regulate the big technology companies. In summary, current policies do not allow effective interventions. Even if they did, such interventions may not be popular.

FIGURE. 13

NATIONAL AUTHORITIES MAY FIND IT HARD TO REGULATE GLOBAL TECH

LACK OF ALTERNATIVES	there are often limited alternatives to global tech products, which are ahead of competitors in innovation and benefit from global scale economies
CONSUMER POPULARITY	many global tech products are highly popular with consumers, which reduces opportunities for restrictive regulation
KEY FOR PROGRESS	use of technologies offered by global tech may also help to drive progress and hence economic growth
BARTER TRADE BUSINESS MODELS	global tech sometimes runs hard-to-regulate business models based on big data barter trade, i.e. consumers give up personal data in exchange for a service or services
GEOGRAPHICAL PRESENCE	global tech has often limited geographical presence in individual countries, which makes it hard to regulate
TRANSPARENCY OF ALGORITHMS	global tech often uses not entirely transparent algorithms to filter and process information – this may have material impact in the real world

Source: Digiteccs Associates

Meanwhile, governments and regulatory bodies have multiple avenues how to intervene in local telecoms. The cleanest way is using regulations based on long-term policies and laws, executed by independent regulatory bodies on a consistent basis. That said, governments often use less systemic and transparent power mechanisms to intervene in telecoms (see Fig. 14).

- Firstly, they make telecoms excessively dependent on certain fundamental privileges, such as spectrum renewals, and take advantage of government's ultimate power to decide about such privileges.
- Secondly, they use the so-called 'prisoner's dilemma' tactics to achieve a certain type of behavior, such as price cuts. This entails providing one player with asymmetric regulatory advantages that encourage such behavior, whereas other players have to follow for competitive reasons.
- Thirdly, governments sometimes use their influence in telecoms as shareholders.

Legality of these tactics depends on specific situations and jurisdiction. However, irrespective of that, such tactics tend to be short-term and non-conceptual. Hence, while providing limited help in resolving the underlying digital policy challenges, they may deter long-term capital investment in telecom infrastructure. To minimize such tactics, a new robust policy framework would help.

ABSENCE OF A DIGITAL POLICY FRAMEWORK MAKES INTERVENTIONS IN TELECOMS OFTEN SHORT-TERM AND TACTICAL AS OPPOSED TO STRATEGIC

FIGURE. 14

GOVERNMENTS USE TOOLS BEYOND STANDARD REGULATIONS TO INTERFERE IN TELECOMS

Source: Digiteccs Associates

Finally, policymakers inadvertently face conflicting interests of different players in different market segments. Fig. 15 shows such potentially different strategic preferences. It is therefore important that any adopted solution is sufficiently conceptual, long-term and consistently enforced to convince the respective stakeholders to play ball and avoid long-lasting regulatory and legal uncertainties, deadlocks, delayed decisions and unhelpful compromises. These are too often seen in digital markets.

FIGURE. 15

POTENTIAL CONFLICTING PREFERENCES OF DIFFERENT STAKEHOLDERS

Source: Digiteccs Associates

	SPECTRUM	SHARED INFRASTRUCTURE	ANTI TRUST	NATIONAL DATA OVERSIGHT
GLOBAL TECH	dynamic	preferred		do not prefer
LOCAL TELCO	private nationwide	often not preferred		may prefer
LOCAL ICT	wholesale	preferred		may prefer
BIG INDUSTRY	private local			
SME			support	
CONSUMER			support	

4.5 SECURITY, FREEDOM, DEMOCRACY, HUMAN CENTRICITY, HEALTH AND SUSTAINABILITY

SECURITY

The overlap between the virtual world and the real world will grow as digital technologies expand. This means that humans will be increasingly dependent on the virtual world for their work, entertainment and everyday life, but also for money, personal and national security, and health. Moreover, digital technologies show a tendency towards centralization in the virtual world, with effects in the real world as well. This, brings a range of new security risks to individuals, linked to for example to:

THE GROWING OVERLAP BETWEEN THE VIRTUAL AND REAL WORLDS BRINGS NEW SECURITY RISKS

- Malicious human intent such as cybercriminals causing economic or physical damage, terrorists using digital technologies, intentional spread of misleading information to cause harm etc.
- Human error including failures of ICT systems due to human errors in design or operation.
- AI impact including situations when AI systems cause harm without easily attributable responsibility.
- Natural reasons including ICT system failures caused by random natural factors, power cuts etc.

FREEDOM, DEMOCRACY AND HUMAN CENTRICITY

Digital technologies are not only capable of disrupting economies, but also the governance of societies. Our current interpretations of freedom, democracy and human centricity in our decision-making may become subject to pressures. There are a number of relevant disruptive risks including the following:

- Disruption of the established media ('fake news'). Power has been shifting away from professionally edited media to social media. At first glance, this leads to de-centralization and empowerment of individuals. However, this trend has also weakened the fundamentally important effects of competition between the established media outlets on public opinion, and hence on democracies. Media power has moved to more opaque social media algorithms, which appear to be promoting extremist and factually incorrect content ('fake news'), or in an effort not to do so, they may subject their content to their own ideological scrutiny. Meanwhile, falling subscription revenue of the established media outlets may adversely affect their editorial independence.
- Disruption of the democratic processes. The above discussed media trends have a direct impact on democratic elections. This is particularly relevant, because social media algorithms are often controlled by global companies, which follow policies formed outside individual nation states. Such algorithms often take advantage of the vast amount of information they have to deliver persuasive messages to their audience. Such algorithms may also be able to predict individual users' voting preferences with a high degree of precision, and then selectively remind individuals to take part in the elections, for example. Another potential challenge to democratic decision-making is linked to the process of voting itself. Any attempts to deploy digital technologies for voting and counting votes, obviously brings major credibility and security risks.
- Disruption of personal life and privacy. Digital tracking of people using smartphones, smart homes, smart cars, smart cities etc. not only enhances our personal life, but it also compromises our privacy and constrains our control over certain decisions, also in the physical world (e.g. car computer overruling or displacing the driver). Some people are more sensitive about this than others. The importance of this issue is further escalated when the adoption of certain technologies are used on people without their consent, their use becomes mandatory by law, or inevitable for practical or social reasons.

PROTECTION OF FREEDOM, DEMOCRACY AND HUMAN-CENTRICITY IS FAR FROM GUARANTEED IN A DIGITALLY DISRUPTED ENVIRONMENT

- Control and red tape enabled by AI. Following on the earlier point, digital technologies open up unprecedented opportunities in regard to surveillance, especially when voice recognition, face recognition and AI are used. The opportunity to automatically collect and process data at low cost (and hence in a large scale) raises a possibility that those in power expand their control via red tape, requiring individuals to provide more specific data, and restraining their freedoms.
- Lack of human centricity of AI robots. Like in social media, robotic AI algorithms may also be opaque and evolve in ways which most humans may not understand and control. We cannot take for granted the fact that such algorithms will act in the best interest of the majority of humans, they will respect legitimate rights of minorities, and honor human society rules and values.
- Disrupting the labor markets by AI. Finally, digital technologies and AI are likely to disrupt the labor market, affecting certain economic freedoms of the workers. Again, it is far from guaranteed that AI will act in the interest of humans.

HEALTH

The digital industries have so far appeared relatively 'friendly' to human health compared to many other industries. A wide range of opportunities are opening for the digital industries to play a role in the prevention and treatment of health problems. That said two issues should be explored.

- Side effects of overuse of digital technologies on humans. These include mental health issues such as addiction and anxiety. Overuse of digital technologies may also curtail other human activities, such as physical exercise and social interaction, which are essential for overall long-term health and well-being.
- Potential impact of wireless radiation on humans and natural ecosystems. Electromagnetic radiation (RF) interferes with living tissues, causing mainly thermal effects (heating of tissues). Regulatory authorities set RF exposure limits at levels which do not cause harm to humans based on the existing scientific evidence. Scientists also claim that within the approved limits, no other (non-thermal or secondary) RF health effects have been proven to cause human health damage. They specifically claim that RF at frequencies used in wireless communications is not powerful enough to damage DNA.

That said, a minority of the science community and parts of the public challenge some of these conclusions. Research about wireless RF has already been conducted for decades, which gives some comfort about safety. However, there is a scope for future research in areas such as: long-term exposure to relatively small doses of RF; potentially different biological responses to RF by different individuals, combined effects of RF and other polluting factors (e.g. food or air toxicity); effects of RF on human microflora; effects of RF on animals and plants; possible effects of new technologies such as beamforming; and effects of a major increase in numbers of connected devices in indoor areas. There is also some scope for a debate about how health effects as such should be defined for the purpose of such studies. The wireless industry has expressed its support for future studies via its association, GSMA.

WHEN RIGHTLY USED, DIGITAL TECHNOLOGIES HAVE LIMITED ADVERSE HEALTH EFFECTS, BUT CONTINUED RESEARCH IS CRUCIAL AS SCIENCE AND TECH EVOLVE

SUSTAINABILITY

Digital industries can provide solutions to a number of sustainability challenges, including energy savings via smart management of various ecosystems, reduction of a need for some physical products and transportation, which can be replaced by digital services.

That said digital industries must themselves address some self-caused sustainability challenges such as:

- Rapidly expanding energy use in data storage and data processing, especially when excessive amounts of data are processed due to misguided ambitions or lack of coordination between different entities.
- Energy use when moving massive amounts of data around the world.
- Additional energy demands linked to an expected substantial increase in connected devices, wireless charging etc
- Energy use from operating unnecessarily overlapping RAN networks, unnecessarily overlapping network technologies (2G, 3G, 5G, 5G), energy inefficient old network equipment and underutilized (excessively dense) networks.
- As already mentioned, RF health impact on broader environmental ecosystems also needs to be further studied.

WHILE DIGITAL INDUSTRIES PROVIDE ENVIRONMENTAL SOLUTIONS, THEIR OWN ENERGY USE MUST BE SCRUTINIZED

5. BROAD-BASED DIGITAL PROSPERITY

5.1. ABOUT BROAD-BASED DIGITAL PROSPERITY

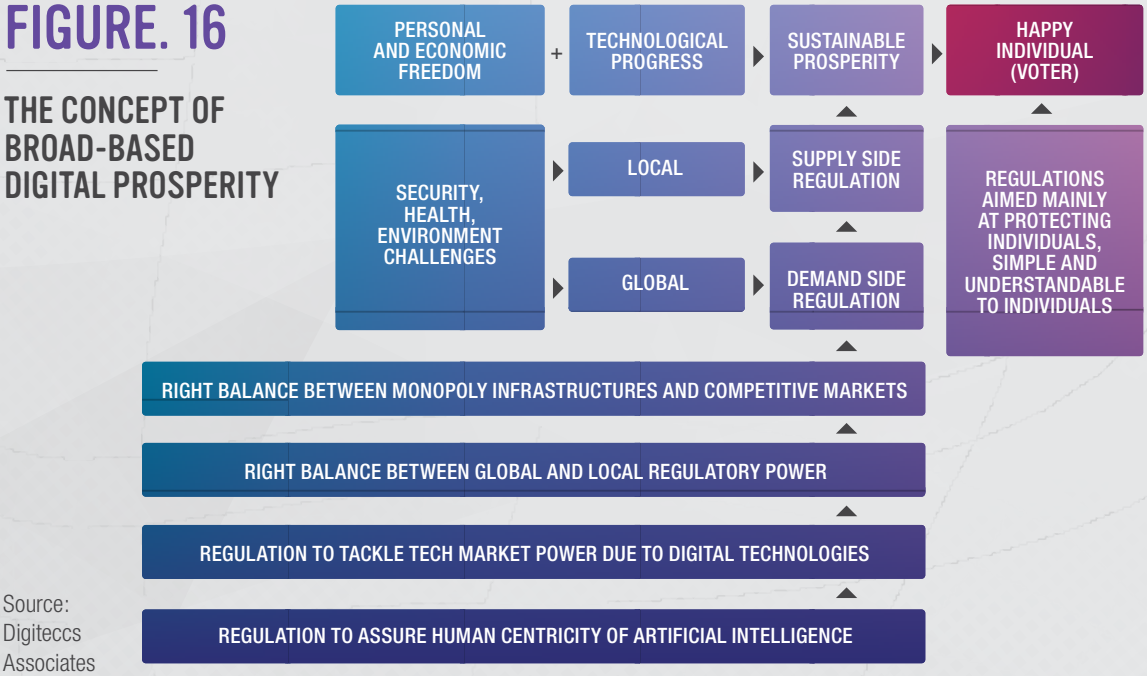
BROAD-BASED DIGITAL PROSPERITY REQUIRES DIGITAL GOVERNANCE, DECENTRALIZATION, DEMOCRATIZATION, OVERSIGHT OF RISKS AND THE RIGHT APPROACH TO MARKET POWER

Our vision of Broad-Based Digital Prosperity is a response to the challenges described in the previous chapter. It is based on our DIGITECCS (digital technology, connectivity and service) thesis, purporting that future economic growth may be to a large degree driven by digital services powered by expanded technology and connectivity. To turn such growth into a broad-based prosperity, as opposed to wealth concentration in the hands of a small number of stakeholders, societies need to:

- De-centralize, 'democratize' and 'de-monopolize' digital service markets by promoting competitive diversity, making it harder for individual entities to disrupt the free markets by gaining a major big data advantage.
- Implement robust governance in data, cloud and digital services, which involves supervision from elected governing bodies, creates conditions for national economic prosperity while protecting society values.

FIGURE. 16

THE CONCEPT OF BROAD-BASED DIGITAL PROSPERITY



Source: Digiteccs Associates

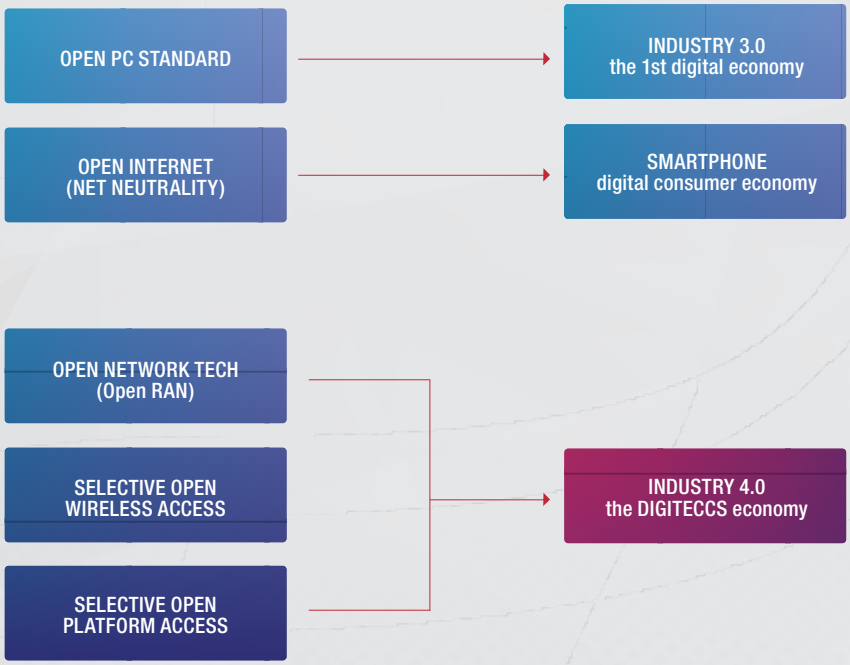
- Tackle adverse security, health, environmental and societal side effects through regulations. When the harm caused by technologies is contained to a specific local area, restrictions should apply to the supply side (e.g. radiation limits for antennas). Otherwise restrictions should apply to the demand side (e.g. restricted use of harmful content, insecure devices and unsafe software etc).
- Where monopolies make better sense, policymakers must build credible long-term frameworks to facilitate them. This can apply in technologies and to networks, as well as data platforms.

5.2 OPENING OF TECHNOLOGY STANDARDS, PLATFORMS AND NETWORKS

One of the main ways to de-centralize, de-monopolize and democratize digital service markets is by opening technology standards, platforms and networks (see Fig. 17). This is not trivial.

FIGURE. 17

HOW THE OPENING OF TECH STANDARDS, PLATFORMS AND NETWORKS LEADS TO PROGRESS



Source: Digiteccs Associates

Proprietary technologies, platforms and networks usually emerge from innovation and investment. While opening can lead to more widespread use of such technologies, platforms or networks, and hence better scale economies with possible win-win outcomes, it may also suppress the ability of specific entities to control their assets. This may in turn adversely impact investments and innovation. Opening is also not binary (open vs. proprietary), but rather a more subtle issue. Each public network, for example, can be seen as being open to a certain degree.

Since proprietary technologies, platforms and network infrastructures are principally owned by private companies, the ultimate choices of how these assets are run should ideally stay in their hands. Unilateral efforts by policymakers to reshape the existing assets towards predetermined outcomes may be hard to execute, face legal challenges, and bring adverse unintended side effects.

However, given their responsibility for creating prosperous conditions and for protecting core societal values policymakers have grounds to make choices, as they did many times in the past, which will partially determine the future shape of certain markets. This way they can also influence the opening of technology standards, networks and platforms, ideally alongside the following principles:

- The respective technology, platform or network layer, which is proposed to be open, is **not subject to major innovation,** it is suitable to a sharing model due to scale economies, it faces limited capacity constraints, and duplication may be counter-productive due to resource, compatability or other reasons.
- Such opening is in the **public interest,** i.e. it is consistent with core societal values.
- **Such opening is ideally adopted on a voluntary basis,** and it attracts cross-industry support. Rather than legislating to open certain technologies, platforms and networks on specific technical terms, policymakers should create conditions under which such outcomes happen through market forces. This can be achieved by creating conditions under which the existing market players act in certain ways, or new entities enter the market with more suitable business models.

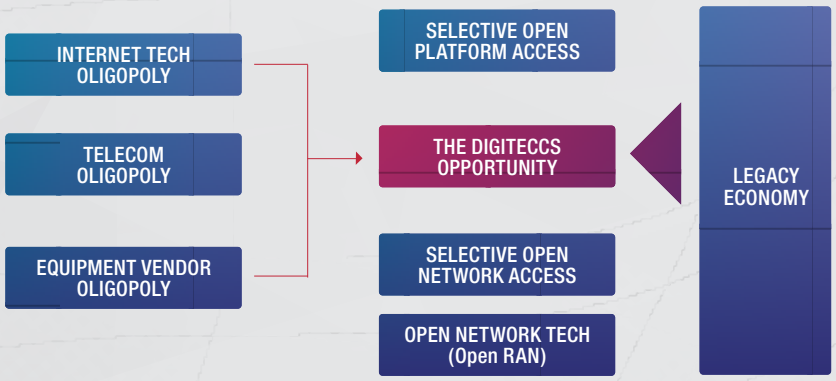
Figs 18 and 19 show how opening can dilute the power of legacy oligopolies in digital services, but also change the way the digital economy works more in favor of local companies. Already implemented or considered examples include:

- Open RAN, meaning virtualized RAN networks built on open source rather than proprietary radio technologies (e.g. Rakuten, the Open RAN Alliance containing the world's major telecom operators including Vodafone)
- Open platforms, including rules imposed either voluntarily or by national policymakers to assure fair functioning and potential interoperability of such platforms (e.g. decentralized data technologies such as blockchain. Also Facebook's Mark Zuckerberg has repeatedly called for regulations of content to reduce the platform's own decisions in some areas)
- Open access tower, fibre and RAN networks (e.g. the tower industry in general, fibre initiatives in Italy and elsewhere, structurally separated networks such as Cetin)

OPENING OF TECHNOLOGIES, PLATFORMS AND NETWORKS OFFERS A SOLUTION TO MANY DIGITAL CHALLENGES, THE IDEA IS NOT NEW

FIGURE. 18

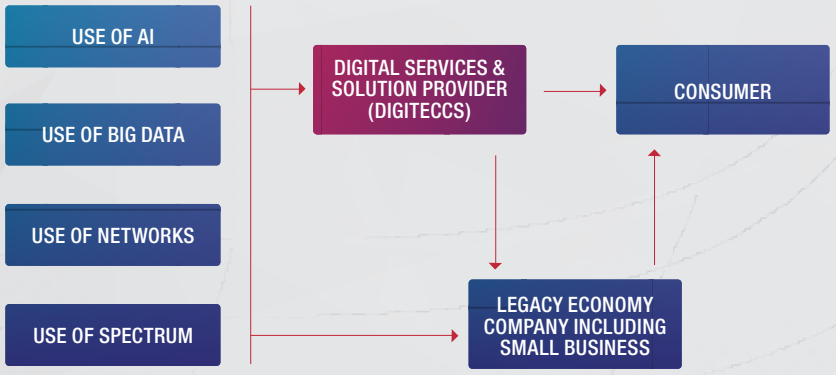
HOW TACKLING OLIGOPOLIES CAN HELP NATIONAL DIGITAL ECONOMIES



Source: Digiteccs Associates

FIGURE. 19

MORE OPEN MODEL FOR PROVISION OF DIGITAL SERVICES



Source: Digiteccs Associates

5.3. RE-ASSESSING WHERE COMPETITION MAKES SENSE

The internet and digital consumer markets were created in the 1980-90s with a liberal and libertarian bias. The emphasis was on one hand on organizing economies around free market principles (capitalism, economic liberalism), on the other hand on sharing information freely and ideally without any rules and boundaries (anarchism, libertarianism). Digital ecosystems have been built in two distinct segments, each following a different approach.

- Capitalism (liberalism) in telecoms. In the 1980-90s telecoms were liberalized. Policymakers ended network monopolies by enforcing competing wireline and wireless networks. At that time, when promising new network technologies emerged, the move appeared sensible. It allowed competitive differentiation between network technologies to drive infrastructure expansion.
- Anarchism (libertarianism) in the internet. Unlike the telecom industry, which has been driven by network competition and where revenue has been derived from the end-users in relatively transparent ways, the internet was built around a notion that information and services are practically free, available to everyone and ideally unconstrained by any rules. Some of these principles were later formally reinforced through net neutrality. That said, the seemingly free service has often been funded from the non-transparent harvesting of data and their subsequent commercial use to influence consumer behavior.

THE DIGITAL ECONOMY HAS BEEN BUILT AROUND THE IDEAS OF CAPITALISM IN TELECOMS AND ANARCHISM IN THE INTERNET . . .

. . . OLIGOPOLIES NEED TO BE TURNED INTO BETTER FUNCTIONING COMPETITION OR WELL-GOVERNED MONOPOLIES

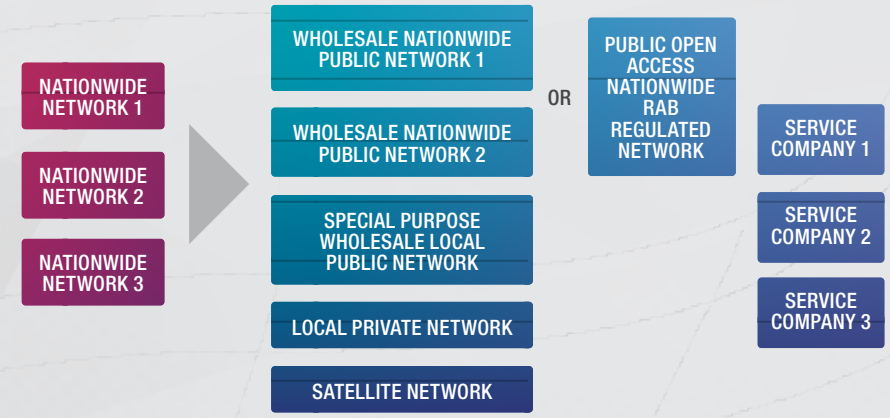
We think that the above-described ideological division within the digital industry is not healthy, natural and sustainable in the long-term. Instead, ideally, we call for a combination of transparent and well-governed monopolies on one hand, and well-functioning competition on the other. Policymakers must be to some degree involved in choosing where monopoly solutions are adopted and where there is room for competition. Global coordination of some of the policies and decisions may be helpful. We are already seeing tendencies towards implementing monopoly-like solutions, for example:

- in network technologies we are already seeing a trend towards open RAN, which would reduce or eliminate competition between different network technologies, effectively commoditizing this market

- in networks, we are seeing a move towards deeper nationwide infrastructure sharing, the wholesale model and consolidation, which leads to reduced competition and even re-creation of monopolies in some cases; new private networks are usually local monopolies by nature
- in platforms, we are seeing unprecedented global market concentration, which is prompting discussions about monopoly regulations

FIGURE. 20

CHANGING COMPETITIVE PARADIGM IN TELECOMS



Source: Digiteccs Associates

5.4. BUILDING STRATEGIC INFRASTRUCTURES FOR DATA AND ENERGY

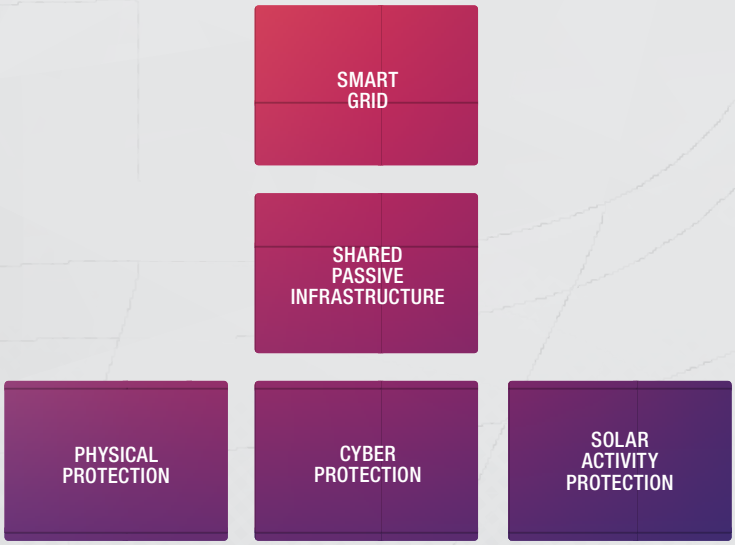
Telecom and digital infrastructures have often been built independently of energy, transport and other infrastructures. However, the growing strategic importance of national digital infrastructures, combined with needs to expand them, often exposes new synergies between digital and other infrastructures, particularly in energy, in two main areas:

- Passive. Extensive new fibre and tower networks will need to be built to operate future wireline and wireless networks. It is likely that utilizing the existing energy and other infrastructures can make such expansion easier, particularly in hard to reach areas. Combining digital and energy infrastructures can also make their physical protection more efficient.
- Active. The energy industry will increasingly need high quality digital infrastructures to manage its smart grid. Active parts of both the smart grid and public digital infrastructures will need to be secured against cyber threats. Finally, disaster management safeguards may need to be put in in place to secure both the energy and digital infrastructures, also against exceptional solar activity.

SYNERGIES BETWEEN DIGITAL AND ENERGY INFRASTRUCTURES SPAN FROM SHARED FIBRE, TOWERS AND CYBERSECURITY THROUGH TO PROTECTION AGAINST SOLAR ACTIVITY

FIGURE. 21

DIGITAL AND ENERGY INFRASTRUCTURE SYNERGIES



Source: Digiteccs Associates

5.5 TRANSFORMING TELECOMS

As previously discussed, modern telecoms have been built around the notion of combining infrastructure and consumer services, and running the resulting entities based on a liberalist notion of competition between multiple networks. Despite its initial successes, this approach has ultimately brought a number of challenges:

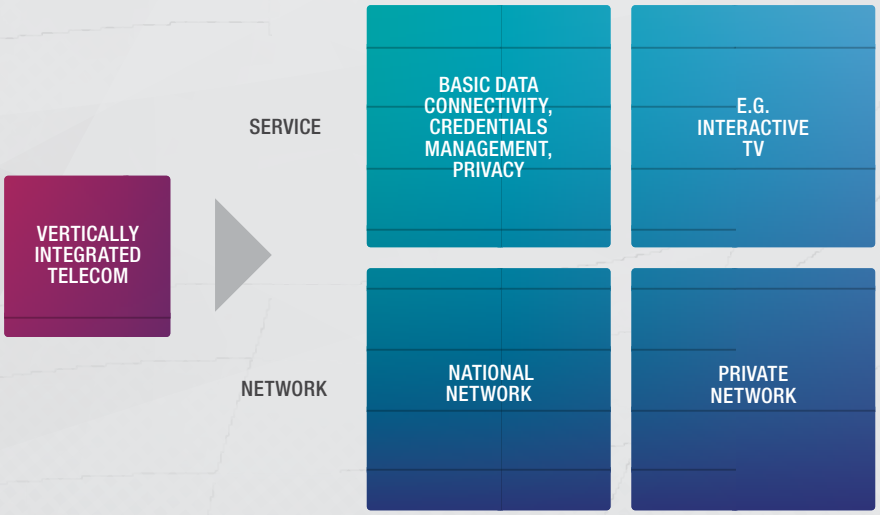
- unique networks and spectrum allocations are often not replicable by competitors, leading to **quasi-monopolies**
- even if technically possible, **infrastructure replication would sometimes be economically wasteful and environmentally unfriendly**
- **telecoms often sideline investment in their consumer and service businesses**, because they see their key economic objective in earning a return on their network investment and retail differentiation may not even help that objective
- the scope of their business often **makes telecoms too complex and subjects them to extensive regulations**, making it harder for them to compete in services
- the capitalist (liberal) nature of the telecom businesses often forces such companies to **engage in not always strategically well thought through ethics-driven PR investments**

FOCUS ON INVESTMENT RETURNS DOES NOT ENCOURAGE VERTICALLY INTEGRATED TELECOMS TO SUFFICIENTLY DIFFERENTIATE SERVICES

Given the described situation, we see a merit in separating telecom infrastructure from services. That said we acknowledge that vertical integration is deeply rooted in telecoms, and transition to the structurally separated model may be complex and take time.

FIGURE. 22

DIVIDING THE VERTICALLY INTEGRATED TELECOM BUSINESSES



Source: Digiteccs Associates

5.6. CREATING EFFICIENT MARKETS FOR BIG DATA

Modern technologies such as smartphones have enabled harvesting personal data in proportions incomparable to anything seen before. This includes deeply personal data about individuals' location, communication, personal contacts, online and economic activity. This is already being extended to include medical data from wearable sensors, but also data from smart homes, cars etc. Corporates often record and store as much data as they possibly can, because they see potential future commercial value in it. Governments, too, find such data valuable, for example for security reasons.

Although businesses are increasingly recognising the strategic importance of big data, the market for big data itself is currently not very transparent and functional. Consumers are often unaware of the scale of data harvesting while corporates are trying to create their own data silos, unable to effectively trade data with their peers. Governments are sometimes left out of some big data segment, unable to access or protect potentially strategically important data.

There are two fundamental ways to look at big data.

- Capitalist/liberal (data is private). Data is a private asset. It is 'created' by private entities and protected by privacy laws. Collection and processing of data about private entities without their consent should be severely restricted by privacy regulations. Private entities including consumers own their data, and they can decide to sell it.
- Anarchist/libertarian (data is public). Data is a public asset. It is in the public interest for data to be available as widely as possible in the best organized way, so that any entities can freely benefit. Users of digital services will practically have to waive most of their privacy rights in exchange for using the services. Protection of privacy in a true sense may not even be possible and most people would not even want it.

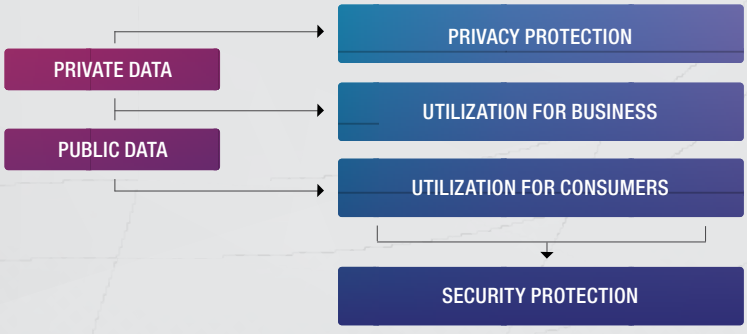
Our societies will have to choose which data they want to treat as private and public. Some cases are relatively simple. For example, personal health records sit well in the private category while published social media posts are naturally public. However, things may get trickier. For example, our physical presence in a specific public location is public information, because we can be identified by bystanders. However, this does not mean that our entire location history is public information. Mass surveillance technologies powered by face recognition and AI can however potentially bridge this gap. This means that we may have to specifically regulate AI that has the ability to turn public data into private data. We will also have to clarify frameworks for harvesting, transmitting, storing, protecting and disposing of private data, and of course trading with such data. Finally, some private data may require special protection.

POLICIES ARE NEEDED TO DEFINE WHICH DATA IS PRIVATE, AND SET RULES HOW SUCH DATA IS HANDLED AND PROTECTED

The GDPR regulation in Europe is the first major attempt to tackle the data regulation challenge. However, to address the essence of the issue societies may have to go beyond dealing with consumer transparency, protection and privacy approvals.

FIGURE. 23

PROTECTION AND UTILIZATION OF PRIVATE AND PUBLIC DATA



Source: Digiteccs Associates

5.7 POLICIES FOR SECURITY, FREEDOM, DEMOCRACY, HUMAN CENTRICITY, HEALTH AND SUSTAINABILITY

SECURITY

Solutions for security can be either market or regulatory-driven. The former is ideally driven by decentralization, democratization and de-monopolization of digital markets to give consumers sufficient and transparent market-driven choices for their security. The latter is triggered in situations when risks for nations, systemic risks, inability of consumers to properly assess the risks or inacceptable health and safety risks create a need for direct regulatory interventions. National governments may conduct such interventions in different ways, for example by:

- banning certain technologies or products
- subjecting certain technologies and services to licensing supervision
- mandating government-provided solutions in certain areas

FREEDOM, DEMOCRACY AND HUMAN CENTRICITY

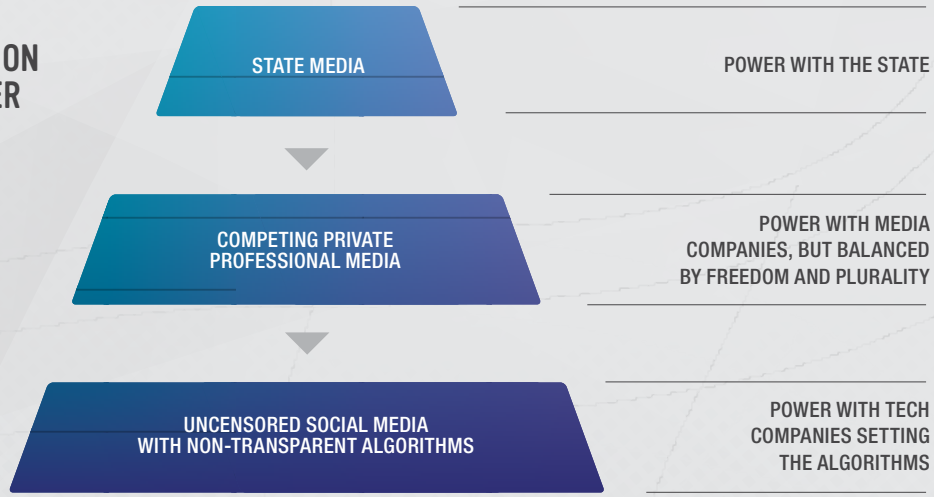
Citizens exercise their freedom and democratic rights in two ways, through their economic activity in free markets and through their voting in elections. Moreover, nation states, which honor human centricity, also try to minimize unnecessary intrusion in peoples' lives. Digital technologies may disrupt mechanisms used by societies to protect freedoms, democracy and human centricity. This may happen for example through:

- reduction of economic choices due to excessive digitally driven market power concentration
- excessive influence of digital algorithms on public opinion, e.g. via social media
- excessive surveillance and red tape enabled by digital technologies

The key basis for a solution is promotion of free market competition in digital markets as well as protection of our democratic mechanisms in the context of tech driven changes. That said, more direct interventions may be necessary to deal with issues ranging from manipulative power of social media and AI algorithms (see Fig. 25), restraining surveillance, red tape or anti human-centric tendencies in AI.

FIGURE. 24

FIG. 24 EVOLUTION OF MEDIA POWER



Source: Digiteccs Associates

FIGURE. 25

POTENTIAL APPROACHES TOWARDS MANIPULATIVE POWER OF SOCIAL MEDIA ALGORITHMS

Source: Digiteccs Associates

Digital technologies will also raise freedom dilemmas, for example:

1. **Use of biometric identification or implanted chips can give humans new freedoms while taking away some of the existing ones.** Such technologies can for example give individuals ability to access certain areas, use certain services or conduct transactions without a need for keys, ID cards, tickets, credit cards and wallets. However, such technologies would further centralize personal data, interfere with privacy and open a scope for discrimination, either intentional or caused by technology failures. There are two solutions. The first one is to strictly assure that individuals have a choice to opt out of using such technologies without incurring major disadvantages. The second one is to subject such technologies to pro-freedom regulation.
2. **The ability of AI to organize our life and work more efficiently temporarily boosts our freedom to choose living and working in superior ways, however over time it may significantly curtail our freedom to opt out of AI advice.** Similar to internet services, major freedom-related problems occur when it becomes practically impossible to opt out of using certain AI services, for example, for legal, practical or social reasons. Again, such cases warrant regulatory solutions, which reflect preferences of the societies.

Finally, to protect human centricity, societies need to be careful about delegating decisions to AI and when they do, establish accountability. Ideally, there should be a cross-society debate about what types of decisions we are willing to delegate to AI, leading to regulations enforcing the right balance of human input in decisions.

USE OF BIOMETRIC TECHNOLOGIES AND RELIANCE ON AI NEED TO BE REGULATED ON FREEDOM, DEMOCRACY AND HUMAN CENTRICITY GROUNDS

SUSTAINABILITY AND HEALTH

Digital industries should pro-actively explore and fund research into sustainability and health impact, both direct and indirect, of their operations, products and services. They should look both at positive and negative impacts. Apart from impacts on human health, research should also focus on health of the ecosystems and energy consumption (CO_2 emissions). Governments should fund independent studies, especially where potentially conflicting interests arise. Potential issues should be addressed through the digital industries' own initiative, if needed, through licensing and regulation, which may encourage certain behaviors, including consolidation. In terms of sustainability, particular attention should be paid to energy consumption for different digital industry and business models.

RESEARCH SHOULD BE CONDUCTED INTO BOTH POSITIVE AND NEGATIVE SUSTAINABILITY AND HEALTH EFECTS OF DIGITAL TECH

6. REGULATORY INTERVENTIONS

6.1 GROUNDS FOR POLICY AND REGULATORY INTERVENTIONS

Societies must always balance freedom and protection of their citizens. Freedom is best achieved through the absence of government intervention except for enforcing justice. Protection however requires policy and regulatory interventions. Below we discuss protection-related reasons for governments to intervene in the real world and contrast them with similar situations in the digital world.

- Defence against common threats. Such services usually cannot be differentiated and provided to specific individuals. Instead, they are provided by governments collectively to the entire society. Examples include national defence, policing, defending democracy via fair elections, epidemic control, disaster management.

  In the digital world, examples include protection against threats to national digital infrastructures including physical damage, sabotage and cybersecurity threats, similar risks to digital infrastructures in strategic industries, defense against certain threats posed by AI etc.

- Universal services. Such services should be made available to all citizens based on agreed nationwide policies. They are usually provided by government entities or licensed entities. Examples include basic healthcare, basic education, electricity access.

  In the digital world, examples may include broadband connection at certain basic specifications, public software applications (e.g. e-government) etc.

- Solidarity. Governments may finance provision of certain services to certain individuals and groups, based on solidarity principles, for example healthcare or social benefits for those unable to work.

  In the digital world, examples include provision of subsidised broadband and potentially also specialized services provided to disadvantaged groups (e.g. digitally powered assistance to disabled people).

- Scarce resources. Nations may consider some scarce resources as strategically important and manage their allocation based on politically established public interest. This includes for example building national strategic oil reserves, management of healthcare-related assets, or management of strategically important land.

  In the digital world, examples include spectrum, network capacity at the time of crises, strategically important data, digital and AI services.

- Market power. Governments may intervene when certain market players reach excessive market power, which distorts functioning of free market competition.

  In the digital world, examples include market power in network technologies, networks, big data, internet data platforms and AI.

- Global economic competition. Within the scope permitted by international trade agreements governments sometimes use interventions such as investments into infrastructures or specific sectors to boost competitiveness of national economies. Some countries also use protectionist measures to create a disadvantage for certain global competitors vs. national players.

  In the digital world, examples include countries subsidising their globally competing digital tech industries, allowing such industries to build excessive market power, or supporting investments in infrastructure. Protectionist measures include for example restriction or taxation of certain products and services. However, there is sometimes a fine line between protectionism, establishing fair conditions for trade and legitimate safety protection.

- Government resourcing. To perform their function, governments need financial resources and powers. The former is obtained mainly via tax revenues while the latter is drawn from the government's ability to legislate, spend public funds and enforce its decisions.

  In the digital world examples include taxes and fees imposed on digital infrastructures and digital service providers; ability of governments to use digital technologies to enforce their power, e.g. via e-government.

REGULATORY APPROACHES FROM THE REAL WORLD SHOULD BE MIRRORED IN THE DIGITAL WORLD

6.2 NEW APPROACHES TO DIGITAL REGULATION

We see the current regulations in the digital world as generally underdeveloped, often lacking a conceptual approach and not always fit for purpose.

This is perhaps unsurprising, because the digital industries have been evolving faster than most other industries. Telecom liberalisations in the 1980-90s, coupled with the rise of wireless networks and commercial use of the internet, brought a notion that the digital industries are best left to relatively unrestricted market conditions.

This is coupled with the fact that policymakers often do not fully understand the nature of data, digital and AI markets, the implication of market power in such markets and the risks that such technologies may pose.

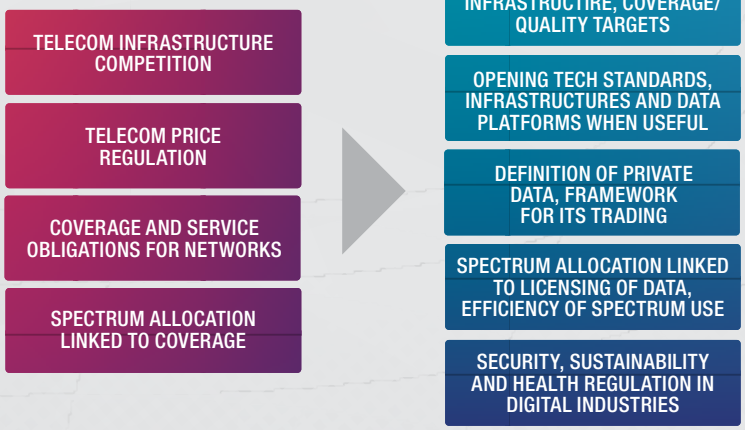
We believe that building such understanding and treating data, cloud, digital services and AI as other goods and services is now very important. In Fig. 26 we show how a regulatory approach should ideally change to achieve this. We see the following policy priorities as crucial.

1. Accepting the concept of strategic shared national digital infrastructures with less infrastructure competition and some degree of government influence over investments.
2. Supporting an industry transformation towards more open technology standards, networks and platforms where this is sensible, while avoiding unnecessary regulatory burdens in digital markers.
3. Clearly defining what is private data and how is it handled and traded.
4. Potentially combining spectrum and data service licensing, with the focus on most efficient use of spectrum and provision of licensed data services.
5. Constantly researching issues around security, sustainability and health implications of digital and wireless technologies, and intervening when necessary.

DIGITAL POLICY FRAMEWORKS MUST ADDRESS THE ISSUES IN DATA, DIGITAL SERVICES AND AI AT THEIR HEART

FIGURE. 26

SUGGESTED CHANGE OF REGULATORY FOCUS IN DIGITAL MARKETS



Source: Digiteccs Associates

7. REFERENCES

1. www.digiteccs.world
2. www.veon.com
3. www.itu.int
4. www.gsma.com
5. www.turkcell.com.tr
6. Re-thinking humanity, James Arbib & Tony Seba, June 2020
7. 21 lessons for the 21st century, Yuval Harari, 2018
8. Touching an intelligent world, global industry vision from Huawei, 2020
9. How to approach 5G policies, Digiteccs and the Czech Ministry of Industry and Trade, Dalibor Vavruska & Petr Ocko, June 2020
10. The re-birth of telecom monopoly, Citigroup GPS report, November 2014
11. The re-birth of telecoms as a new digital industry and similar reports, Citigroup GPS report, October 2016
12. Disruptive Innovations VI, Citigroup GPS report, August 2018
13. 5G Observatory Quarterly Report 7, IDATE Digiworld, April 2020
14. 5G and the future of security in ICT, David Soldani, Huawei, 2019
15. The mobile economy 2020, GSMA
16. 8 ways the telecoms industry can help keep everyone connected, opinion, ITU article by Tomas Lamanauskas, 2020
17. Freewill vs determinism. Simply Psychology, McLeod, S. A., 2019
18. Greed is Dead: Politics After Individualism, Paul Collier and John Kay, 2019

DIGITECCS

NOTES

DALIBOR VAVRUSKA

For over 25 years, Dalibor Vavruska has helped investors, companies and policymakers to understand the communications and technology industries. The work of his teams has been consistently top-rated in prestigious international investor surveys, with investors highlighting the quality of the predictions and the unbiased approach. Dalibor's research on the digital transformation of telecoms and communications infrastructure monopoly in recent years set the agenda for the global telecoms industry.

He was also involved in some of the world's most innovative, successful and trend-setting telecom transformation stories, such as the digital transformation of Turkcell, structural separation of O2 Czech Republic and the formulation of the EU's Electronic Communications Act. Following long stints at Citibank and, before that, at ING and other leading banks, he founded Digiteccs Associates Ltd to help various stakeholders to achieve their objectives while building broad-based digital prosperity. Dalibor, a graduate mathematician and MBA, is a frequent speaker at international TMT events. He has also helped to introduce various TMT companies to the stock market in Europe, Asia and Africa.

THE D-NA MODEL IS A UNIQUE SYSTEMIC CONCEPT FOR APPROACHING NEW TRENDS IN DIGITAL TECHNOLOGIES. IT GUIDES POLICYMAKERS, REGULATORS AND ALL DIGITAL ACTORS HOW TO BEST COOPERATE AND DEVELOP DIGITAL ECONOMIES AND SOCIETIES BASED ON HUMAN RIGHTS, DEMOCRACY AND FREE MARKETS.

Petr Ocko, Deputy Minister of Industry and Trade responsible for digitalization, Czech Republic

A MUST-READ FOR ALL PLAYERS ACROSS THE TECH LANDSCAPE, MOST NOTABLY FOR TELECOM COMPANIES IN SEARCH OF WAYS TO UNLOCK THE HIDDEN VALUE OF THEIR CONSIDERABLE CUSTOMER FOOTPRINTS, AS WELL AS FOR GOVERNMENTS TRYING TO FIND THE MOST APPROPRIATE METHODS TO REGULATE EMERGING CHALLENGES AROUND DATA SOVEREIGNTY.

Kaan Terzioglu, co-CEO of VEON, a leading global mobile services operator, and winner of the GSMA's Outstanding Contribution to the Mobile Industry Award for 2019, Netherlands

WHILST I MAY NOT AGREE WITH ALL PARTICULARS, SUCH AS THE IMPORTANCE OF BLOCKCHAIN, AND DESPITE THE SOMEWHAT HEAVY JARGON, I FIND THIS FIRST OUTLINE OF A STRUCTURED APPROACH BY OUR SOCIETY TO THE NEW DATA AND AI DRIVEN ECONOMY A THOUGHT PROVOKING READ.

Miroslav Singer, Chairman of Generali Česká pojišťovna supervisory board, former Governor of the Czech National Bank, Czech Republic

THE WORLD IS ON A CUSP OF MAINSTREAMING THE NEXT GENERATION NETWORK ARCHITECTURE WHICH WILL CONCOMITANTLY ELEVATE APPLICATIONS IN RELATION TO BIG DATA ANALYTICS, AI AND ML TO THE CENTRE STAGE FOR BOTH PUBLIC AND PRIVATE SECTOR ORGANIZATIONS. IT IS IN THIS CONTEXT, WITH DATA BEING NEW CURRENCY, THAT THE PROPOSED DIGITAL NATION MODEL IS A CRITICAL WHITE PAPER. IT IS AN IMPORTANT CONTRIBUTION TO INFORM A NEW REGIME FOR DATA GOVERNANCE THAT IS NEEDED AT BOTH THE STATE AND CORPORATE LAYER.

Shaun Pather, Professor of Information Systems, and ICT Policy Specialist, University of the Western Cape, South Africa

DALIBOR'S LATEST PUBLICATION EXTENDS HIS DIGITECCS CONCEPT TO DATA REGULATION AND POLICY. IT IS A TIMELY, INFORMED, AND ABSORBING READ FOR ALL OF US WITH OUR BURGEONING DATA FOOTPRINTS. IMPLEMENTING HIS GOVERNANCE FRAMEWORK WOULD REQUIRE OVERCOMING CHALLENGES SUCH AS AGREEING A GLOBAL APPROACH TO DEAL WITH THE PREDOMINANTLY US AND CHINESE TECH BEHEMOTHS, ASSIGNING OWNERSHIP TO ONE'S DIGITAL FOOTPRINT AND CLASSIFYING SOME DATA TYPES FOR LICENSING.

Glen Prentice, Investment Portfolio Manager (has worked at Bank of New York Mellon, JP Morgan and sovereign wealth funds), UK

VERY WELL FORMULATED, ENCOMPASSING OVERVIEW AND SUGGESTIONS FOR DIGITAL GOVERNANCE FRAMEWORK. IF WHAT'S BEING SUGGESTED IS EXECUTED, THERE IS FINANCIAL POTENTIAL FOR BENEFITS TO BOTH, THE POLICY MAKERS AND PRIVATE SECTOR IN CREATING NEW JOBS, NEW INDUSTRIES, BETTER PROTECTION FOR SENSITIVE DATA, AND MARKET EFFICIENCY FOR BIG DATA. DALIBOR'S THINKING FOR DATA GOVERNANCE HAS RESEMBLANCE WITH THE TELECOMMUNICATIONS ACT OF 1996, THAT PROVIDED WAYS TO STIMULATE PRIVATE INVESTMENT, PROMOTE COMPETITION, AND GIVE USERS SUPER-HIGHWAY WITH STATE-OF THE- ART TECHNOLOGY.

Dmitry Kononov, former management board member of Megafon, a leading Russian wireless operator, US

DIGITECCS

ISBN 978-80-270-8646-7

INFO@DIGITECCS.WORLD
WWW.DIGITECCS.WORLD