CEPS TASK FORCE WORKING GROUP REPORT

THE DIGITAL TRANSITION

Towards a Resilient and Sustainable Post-Pandemic Recovery

AUTHORS

Andrea Renda
Rosanna Fanni
Lorenzo Pupillo
Carolina Polito

Task Force Working Group Report

The Digital Transition

Towards a Resilient and Sustainable Post-Pandemic Recovery

Authors:
Andrea Renda
Lorenzo Pupillo
Rosanna Fanni
Carolina Polito

With support from:

Centre for European Policy Studies (CEPS)
Brussels

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229.39.11
e-mail: info@ceps.eu
internet: www.ceps.eu

Contents

INTRODUCTION

The digital transformation is undoubtedly a key element of the new industrial strategy for Europe and, together with the Green Deal, part of the 'twin transition' underpinning the European Union's overall growth agenda. The European Commission, led by Ursula von der Leyen, has placed significant emphasis on the need to make Europe fit for the digital age. This is also reflected in the decision made by the EU institutions to allocate €143.4 billion to single market, innovation and digital programmes in the Multiannual Financial Framework 2021-27. High expectations are placed on the potential for the digital transformation to relaunch Europe's industrial leadership over the coming decade. At the same time, the Covid-19 pandemic has accelerated our transition to the digital environment and raised fundamental questions on technological sovereignty, sustainability, cybersecurity and resilience, as well as social inequalities.

Binding and non-binding digital policy initiatives are mushrooming: the Artificial Intelligence (AI) Act, the data strategy, the Digital Services Act and the Digital Markets Act, among others, add to existing frameworks such as the General Data Protection Regulation (GDPR), showing the complexity and interwovenness of markets, networks, infrastructure and people. A suitable approach to the governance of data spaces, the regulation of AI, the speedy and sustainable deployment of the Internet of Things (IoT) and the edge/cloud layer, and even 'getting the science right' on 5G and cybersecurity, are all essential building blocks of a competitive and sustainable Europe for the coming decade.

To address key areas of the digital technology stack in Europe, this Working Group convened three high-level discussion meetings between January and March 2021:

- Meeting 1, "Speeding up the rollout of 5G and other forms of connectivity in Europe: what are the options?", addressed the elements of a 5G rollout in light of other networks and resources, and also considered health, environmental and cybersecurity risks.

- Meeting 2, "Artificial Intelligence and Industrial Transformation", assessed the opportunities and steps towards enabling AI technology as a "force for good", especially in facing climate change and empowering the workforce in digitally enabled work environments.

- Meeting 3, "The edge/cloud layer, data spaces and the future of GAIA-X: anatomy of Single Market 2.0", addressed whether – and how far – the current data strategy enables interaction and flows of non-personal data in its single market, and the role that emerging data spaces and the EU-led GAIA-X project can fulfil.

Ultimately, in framing the digital transformation as a desirable objective, the Working Group asked how far the various modes of connectivity in question could help the EU to achieve its competitiveness, resilience and sustainability targets. The subsequent recommendations made by the Working Group address the potential of these digital areas to effectively make the twin transition a success for Europe's industrial future.

1. ENSURING A SPEEDY, BALANCED ROLLOUT OF CONNECTIVITY TECHNOLOGIES

R1. Evaluate the 5G rollout in relation to the territory and the broader mix of possible technology solutions.

According to the Commission Communication on the 2030 Digital Compass, by 2030 all European households should be covered by a Gigabit network, with all populated areas covered by 5G.1 The latter, if rolled out properly, is expected to provide ultra-low latency and increased capacity for high bandwidth data streams. The Covid-19 pandemic and the associated demand for greater bandwidth from videoconferencing and video streaming, among other things, have further accelerated the debate on infrastructure investments and a regulatory framework to meet the increasing network demand.

However, it is still unclear as to how and to what extent 5G will be integral to the EU industrial strategy and Europe's digital future, and how it should be integrated with other connectivity technologies. While mobile communication technologies have improved dramatically over previous generations, and despite the perceived benefits of adopting 5G, further improvements might be hard won. Enhancements become expensive because 5G implementation requires many more antennae at the base station and in the device, as well as many more small cells (Webb, 2017). This, in turn, will cause subscribers to increase their spending significantly.

Moreover, so far, the 5G market appears to still be mostly supply driven, and policies to promote the demand side will thus be critical to guarantee the sustainability of investment and allow business users to exploit the potential of enhanced connectivity. Manufacturers are relying on the rollout of 5G to provide a boost to their revenues (Webb, 2017). Indeed, the decline in sales of previous-generation technologies is resulting in global suppliers increasingly pressuring the market to introduce new technologies, hoping that consumers will be willing to pay for them. However, we are yet to see a significant 'demand pull' that could assure sales and profitability in business models. Mobile network operators (MNOs), who should in principle be shouldering most of the upfront costs, are currently suffering limited capacity to invest in new technology and infrastructure, as their returns on investment in 3G and LTE-A (4G) are still being recouped. Furthermore, there is a lack of investment in 5G as investors are uncertain about its commercial value and the time that will be needed to propagate the network. If they do invest, they will need to seek member state and EU financing, as future bank covenants may be limited. The availability of recovery and resilience funds can certainly facilitate investment. Nevertheless, it is essential to avoid investment when the underlying business case is weak, and when 5G is not the most cost-effective solution.

At the same time, 5G is a long-term (almost a decade) plan, rather than a short-term opportunity. It is important to ensure that, by the time the technology is mature, its appeal to market players is still strong, as other technologies are already becoming available. It is indeed becoming clear that the technology will take much longer to perfect than earlier generations. China, for instance, sees 5G as at least a ten-year programme, perhaps much longer, before it is fully operational and rolled out nationally. This is because the technologies involved in 5G are much more complex (Webb, 2017). For example, propagation patterns in the field, which can result from active antenna systems and their feedback loops, are still only partly understood today. Europe's ability to meet this demand would be influenced by its ability to navigate the global geopolitical crossfire in the supply chains for 5G – characterised by great interdependence and highly specialised global production – and in other competing technologies.

In this context, the Task Force recommends that the EU adopt a much more nuanced approach to 5G, and acquire a thorough understanding of the mix of complementary technologies needed to fully achieve the connectivity goals for the digital decade. 5G capacity, speed and service availability need to go hand in hand with cloud and edge services and infrastructures. Yet the business case for 5G should also be evaluated against the development of future technologies such as what might be termed '6G', including edge nodes, in order to avoid the rapid obsolescence of the EU's technological targets and ensure their coherence with one another. For example, in its Communication on the Digital Compass, the EU states that at its proposed level of ambition, by 2030 "10,000 climate-neutral highly secure edge nodes[2] [will be] deployed in the EU, distributed in a way that will guarantee access to data services with low latency (few milliseconds) wherever businesses are located". In this respect, a more thorough understanding is needed of whether meeting this target would challenge the business case for 5G.

Careful evaluation of the conditions that must be met for the 5G rollout to be the preferred choice is essential, especially in the context of the National Recovery and Resilience Plans. Comparative analysis should be carried out with other solutions, especially for IoT applications in homes, public spaces such as railway stations and metros, industrial applications and smart cities. For these locations, Wi-Fi in unlicensed spectrum bands (e.g. at low 6GHz) and dedicated radio technologies for real-time control systems (e.g. ZigBee) are available and attractive. The EU should also start analysing the transition from 5G to 6G, building business cases based on sensible use and realistic costing (e.g. a revised frequency allocation process).

Overall, in deploying 5G, more attention should be devoted to:

1. Embedding cybersecurity in network design and management architecture, prioritising the security and confidentiality of data flows.
2. Smart policies for radio frequency allocation, prioritising cost-efficient range and effective building penetration, and minimising high-power operations and intense beamforming.
3. Sustainability, by ensuring low-power and low-energy consumption operation and connectivity.
4. Quality of service and resilience, through uninterruptible operations with suitable redundancy for continuity of critical infrastructure. Moreover, future 5G releases may incorporate improved broadband mission-critical service for public protection and disaster relief emergency services.
5. Avoiding dense (urban) networks with tens of thousands of base stations for a city, bearing in mind site availability and planning permission difficulties, plus the environmental challenges posed by backhaul cabling/microwave line-of-sight congestion, rejection of non-aesthetic designs and power supply complications.[3]
6. Societal aspects: EU citizens deserve relevant, up-to-date and evidence-based information on the health impact of 5G.

Box 1. 6G technology[4]

As the Finnish 6G Flagship's White Paper stresses, "it is not clear yet what 6G will entail". The paper nevertheless describes some elements of the future "ubiquitous wireless intelligence". It suggests a move towards a "6G Humanity" following the 2016 United Nations (UN) 17 Sustainable Development Goals (SDGs), and claims that "6G will require a substantially more holistic approach to identify future communication needs, embracing a much wider". The Hexa-X has similar goals to help address the UN and European SDGs, to shift the "network design paradigm from mainly performance oriented to both performance and value oriented". NTT Docomo's White Paper (2020) mentions the "resolution of social issues/human-centred value creation". While noting that "the fundamental architectural and performance components of 6G remain largely undefined", Saad et al. (2020) hold that the 6G vision will be driven by a diverse portfolio of applications, technologies and techniques.

6G networks are expected to have faster data transmission speeds and the ability to connect to multiple devices simultaneously on a greater scale, as well as featuring extensive security measures and reduced power consumption. According to the International Telecommunication Union Working Group (ITU WG), the new generation will be based on entirely new technologies, in both hardware and software. This means that it will need to be interoperable with the current and forthcoming generations and new formations of space networks. For vertical applications, hugely varying system requirements, such as massive broadband, ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC) and extreme power efficiency, mean many solutions will be required. Future networks will bring a disruptive change to infrastructure owners, IoT equipment vendors and manufacturers of mobile handsets. "The 6G network is likely to be a concept, a virtual one, and not a 'real' network you can put a boundary around" (Saracco, R., EIT Digital, quoted by Hayes, 2020). The Hexa-X document notes that it will aggregate multiple types of resources in an enormous digital ecosystem "and eventually create a single network of networks".

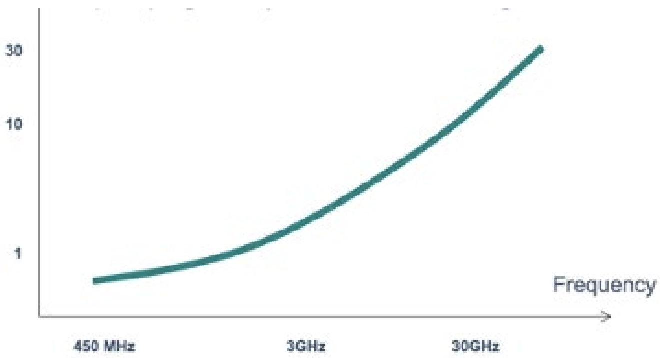
R2. Encourage infrastructure sharing.

5G coverage is expected to evolve gradually, from non-standalone infrastructure, where the radio access interfaces will be the present 4G-LTE as the core infrastructure, including new 5G-NR components, to standalone 5G. The latter in particular requires substantial investment, as the core network must be upgraded (Forge and Vu, 2020) based on cloud services and virtualisation, which are incompatible with the 4G-LTE currently in use.

Potential business models for 5G range from the traditional MNO ownership model, to a shared network infrastructure, to vertical sharing wholesale infrastructures and services. Notably, the current MNO-led business model may be challenged in relation to its costs. As such, new models may emerge for alternative forms of network ownership and operations.

As mentioned, the implementation of microcells to support 5G mmWave services has high costs, potentially limiting return on investment (Moazzamipeiro, 2020). With higher frequencies and shortened ranges, base stations will be packed more closely into an area in order to ensure full coverage of the signal. Ranges of 20-150 metres may be typical, giving smaller coverage areas per 'small cell'. A cell radius of 20 metres implies about 800 base stations per square kilometre (Blackman and Forge, 2019). A shorter range implies more base stations and higher cost, as shown in Figure 1.

Figure 1. Economics of 5G: the cost of a national network is set by the frequency used



Source: Simon Forge (2020), first meeting of the Task Force.

The huge investment required for network deployment, coupled with the ambitious expectations held by public authorities and consumers regarding rollout timing and coverage, will be impossible to achieve without infrastructure-sharing agreements. Likewise, **infrastructure sharing is key to promoting business sustainability, improving the efficiency of energy consumption and reducing environmental impact**.

Sharing may take different forms, such as shared radio access networks (RANs) including spectrum, shared permanently or dynamically. It can also include the passive assets of network environment base station sites, towers with power supplies, and ducts and wayleaves for backhaul where appropriate. Sharing will enable new investment and ownership models that move away from the MNO-centred model to industrially suited paradigms and wider market access for new players. Thus, wholesale networking infrastructures for use by multiple mobile service providers could be considered.

R3. Carefully analyse the technology mix in non-dense urban areas.

According to Daly et al. (2020), 5G networks in Europe can deliver approximately €210 billion in benefits at a cost of approximately €46 billion (4.5 benefits to costs ratio). To exploit these expected benefits, however, the EU must successfully assess which use cases would be best accommodated by the implementation of the 5G network, and which would benefit from the adoption of alternative technologies.

A case in point is rural areas. The extreme densification and short-haul small-cell ranges necessary to achieve 5G will generally make it usable only in dense urban scenarios. In rural areas where the digital divide is most common and requires the most effort to overcome, 5G will not be the most viable solution. In most rural locations, fibre optic networks might indeed represent a better solution than 5G.[5]

Furthermore, despite the potential of microcells to facilitate entry by local and specialised providers, 5G might strengthen existing monopolies or oligopolies.

Micro-licensees may have to pay high charges to incumbent competitors in their area for backhaul or middle mile connectivity. Furthermore, if the spectrum is auctioned, the result may perpetuate the dominance of incumbents, further impairing the affordability of the technology for rural users (Moazzamipeiro, 2020).

Delivering enhanced coverage in a number of known problematic locations would generate greater value for the economy while meeting the demand of consumers. The outbreak of the Covid-19 pandemic has shown the urgency for a universal footprint of the infrastructure, as well as the corresponding need to be imaginative about the required technology mixes. As such, increasing long-term R&D efforts in *all* technologies for connectivity solutions should be promoted to ensure consistent connectivity and adequate coverage in rural areas, at a reasonable cost. This may include research into low-Earth-orbit solutions as part of a global initiative, with due consideration for European solutions.

R4. Address the risks associated with the 5G rollout effectively.

The deployment of 5G should be accompanied by a series of reflections on the related risks, especially in terms of health, cybersecurity, privacy and sustainability.

Health risks

In terms of the impact on health of mobile radio technology, concerns have been raised about the potential negative effects of being exposed to radiofrequency electromagnetic fields on both humans and wildlife (SCHEER, 2018). While the International Commission on Non-Ionizing Radiation Protection (ICNIRP) issued guidelines in 2010 for limiting exposure to electric, magnetic and electromagnetic fields (EMF), it is currently not possible to accurately simulate or measure 5G emissions in the real world (Blackman and Forge, 2019).[6]

Further independent research and closer collaboration with competent health and public safety authorities should be promoted, in order to assess the impact of this technology and potentially help dissipate over-alarming or inaccurate analyses on 5G deployment. In particular, the EU should support research into signal processing and radio physics, especially multiple propagation unknowns (e.g. measuring and controlling RF-EMF exposure with MIMO at mmWave frequencies for active antenna systems).

Cybersecurity and privacy risks

Several cybersecurity risks related to 5G deployment have already been identified by the EU Network and Information Systems (NIS) Cooperation Group (2019). Among these, 5G presents an increased attack surface, consisting of potential vulnerabilities in the software; problems of sensitivity and interoperability at the hardware level and increased exposure to attacks due to the dependency of network operators on third-party suppliers or manufacturers. Furthermore, 5G might exacerbate security risks when integrated into legacy networks (3G and 4G), as well as contributing to the escalation of trade issue with suppliers of key infrastructure (such as Huawei).

In this context, the EU should promote a reliable multi-tiered approach to cybersecurity, with adequate safeguards to protect information through system hardware and software design. The EU 5G security toolbox provides a valuable risk-based approach for evaluating 5G deployment. However, the EU needs to harmonise its assessment of and response to the risks stemming from third-party suppliers. It should also encourage cyber-risk diversification by requiring that every portion of the network has multiple vendors. An initial and periodic security assessment of each participating entity could also be envisaged.

The rollout of 5G will also require an assessment of the privacy risks. According to the latest GSMA report on 5G and data privacy (2020), "while 5G represents a significant shift in the use of mobile networks, existing data privacy regimes already address a wide range of uses of data collected through apps, mobile device operating systems, social media, websites and network operators, and are likely to be sufficient to address the use of new 5G capabilities within the online ecosystem".

Nonetheless, with 5G the exposure of the personal world to the public access world will rise from 100Mbps to 1-20Gbps per second. Hence, the risk of personal information being leaked is considerably higher and might require ad hoc regulatory intervention.

Environmental risks

According to GSMA (2019), **5G might represent an enabler for carbon emission reductions**. In an industrial manufacturing setting, for example, the use of mobile technology for storage and inventory management could "reduce the overall level of inventory and area needed, increasing efficiency and decreasing energy use for lighting and cooling". Similarly, "mobile technology could enable farmers to better regulate and remotely monitor irrigation and soil conditions allowing for more efficient land use".

Nonetheless, other projections are expecting that **with the adoption of 5G, industry power consumption will rise to approximately 1.5 times its current level**. By way of example, in China, where the government is mandating the 5G rollout, MNOs are seeking government aid to pay 5G electricity bills because the bills are higher than the MNOs' margins. While asking governments to subsidise electricity bills does not represent a sustainable solution, the Task Force recommends that the Commission provide guidance to member states on the conditions and targets to be met for energy-efficient 5G deployment, consistent with the UN SDGs and the Green Deal. Energy performance and sustainability goals need to be aligned with financial and operational objectives.

Greater renewable energy capacity and improved grid flexibility and storage will be necessary. The growing number and size of 5G base stations will require more efficient cooling systems, which should be powered by renewable energy. Microgrids could also be a helpful tool in the decarbonisation of energy networks. This should be complemented by research on biodegradable sensors to reduce, reuse and recycle hazardous material that cannot yet be substituted.

2. ARTIFICIAL INTELLIGENCE AND INDUSTRIAL TRANSFORMATION

R5. Promote human-centric, sustainable and resilient AI technologies.

The development of AI in key EU sectors such as machinery, transport, robotics and manufacturing, and healthcare, combined with a robust oversight framework, is the basis for a European AI ecosystem that delivers on a more sustainable and prosperous future. To this end, in January 2021 the Commission published its vision of Industry 5.0, an approach to replace the current shareholder primacy with a stakeholder-centred value concept. The strategy recognises the power of industry to achieve societal goals beyond jobs and growth to better blend social and environmental European priorities with technological innovation. Industry 5.0 is expected to rely on six key pillars: (1) individualised human-machine interaction; (2) bio-inspired technologies and smart materials; (3) digital twins and simulations; (4) data transmission, storage and analysis technologies; (5) AI; and (6) technologies for energy efficiency, renewables, storage and autonomy – benefiting investors, workers, consumers, society and the environment.

An important element of the Industry 5.0 concept is that technology serves people, rather than the other way around. To achieve this vision, a fundamental shift from the current 'platform worker model' towards a future-proof ecosystem for the workforce is required. **Industry 5.0 unites three constitutive elements: human-centricity, sustainability and resilience**. This includes measures towards the intelligent redistribution of tasks between humans and robots/AI systems, up- and re-skilling initiatives, and awareness-raising measures about the risks associated with AI. It also entails incentivising and developing educational trajectories, guidelines and tools for professional and technical staff under the notion of cooperative responsibility, an intuitive and accessible user interface design, and improved mental health support. These ambitious objectives should be implemented in a way that ensures that all EU regions, including those grappling with digitalisation, benefit equally from the Industry 5.0 vision.

As a general-purpose technology, AI can be used for both commendable and less desirable purposes. It is fair to say that so far, the potential of AI as a force for good has not fully materialised. Modelling techniques and connected infrastructures have outstanding potential to support resilience and economic, social and environmental sustainability. A range of monitoring, control and prediction systems in urban contexts, connected cities, transportation systems, energy, weather and biodiversity analysis demonstrate the outstanding potential of AI to achieve **environmental sustainability**, in particular to meet the SDGs. A flagship project in this regard is the **EU Destination Earth (DestinE) initiative, which will contribute to the Commission's Green Deal and digital strategy**. The construction of a digital twin on "weather-induced and geophysical extremes" and "climate change adaptation" is part of a high precision digital model of the Earth to monitor and simulate natural and human activity, and to develop and test scenarios that would enable more sustainable development and support European environmental policies.

The potential of AI systems to protect the planet and create more habitable spaces for citizens can support the EU in meeting its ambitious goal of becoming the world's first climate-neutral continent by 2050. This goal can only be fully achieved, however, if actions are combined with modernising the EU economy and society and re-oriented towards a just and sustainable future. Research and innovation are considered as driving these transformative changes, for instance to reach climate neutrality and ensure an inclusive ecological and economic transition. Both the Horizon 2020 and the 2021-27 Horizon Europe programmes are closely linked to these objectives insofar as they seek to leverage national public and private investment specifically for **innovation, technology, sustainable solutions and disruptive innovation**. Over 35% of the Horizon Europe budget alone will be spent on reaching the 2050 climate objectives through climate-friendly technologies.

This Working Group recommends linking EU funding (e.g. via the Recovery and Resilience Facility) to research and innovation on AI to support solutions that are consistent with the overall goal of making industry more human-centric, resilient and sustainable, in line with the Industry 5.0 approach. Human-centric AI is already at the centre of the recently proposed AI Act. It should now be mainstreamed into national AI investment, especially in industrial ecosystems, as well as into the forthcoming European Alliance for industrial data, cloud and edge, the public-private partnership (PPP) on AI, and other forms of EU funding of AI solutions applied to industry. In particular, research and innovation on 'embedded AI', coupled with more decentralised infrastructure and data storage, and technological solutions aimed at protecting privacy and industrial data, can ensure that the EU promotes an approach to AI that is consistent with its values and overarching goals. When monitoring the industrial strategy, this may entail the use of ad hoc indicators (see also R.6 "What gets measured gets done: choosing future-proof indicators for systemic transformation" in the CEPS Industrial Policy Task Force executive summary).

R6. Prioritise sustainable and decentralised technological solutions.

Depending on how it is implemented, AI and other forms of connectivity can be either a blessing or a curse for sustainability. There is ample evidence of the positive impact that AI can have on energy efficiency, but at the same time some advanced AI techniques are energy hungry. The European digital strategy already recognises this tension and sets the goal of achieving climate-neutral, highly energy-efficient and sustainable data centres by no later than 2030. The EU Green Deal also announced measures to improve the energy efficiency of the information and communication technology (ICT) sector itself, from broadband networks to data centres and robotics devices.

Yet, **the environmental footprint of data centres and algorithmic training techniques** challenge these ambitious objectives. As such, a recent European Commission-led study concludes that, while edge data centres accounted for 2% of the energy used by data centres in 2018, this share is expected to rise to 12% by 2025. This reflects a growing trend towards edge computing because of increasing digitalisation and the associated need to capture, transfer and process more and more data. The study concludes that both existing and new policy instruments need to be established to reach the 2030 European digital strategy targets. It further finds that while sustainable computing has been promoted by the EU, "energy-efficient cloud computing is in general not tackled on national political agendas, nor in EU legislation" (p. 143). Furthermore, in some of the core elements constituting AI – computer networks, data transfers and coding – "little to no evidence is available for energy-efficient cloud services [...] the only examples have been found in research, but have never been commercialised" (ibid.). This shows that the transition to energy-efficient and future-proof deployment of AI can only succeed with policy intervention.

Another issue highlighted in the EU Green Deal is the **lack of public awareness** and transparency on the environmental impact of digital technology and electronic communication. As highlighted in the Industry 5.0 vision, only 12% of secondary raw materials and resources are brought back into the economy. So-called take-back schemes for digital devices are one example of a joint effort, in which companies and private stakeholders will play a crucial role to incentivise the green transition in the EU. Supporting legislation includes the EU code of conduct on data centre energy efficiency, and the forthcoming reviews of the Ecodesign Regulation on servers and data storage products and the Energy Efficiency Directive. This shows the urgent need for strategic guidance if the EU is to meet its goals in terms of climate neutrality and sustainable computing.

To ensure consistency with EU sustainability goals, the **criteria set forth by the European Green Deal should be fully applied to AI deployment projects,** thus ensuring the use of renewable energy in data centres, the adoption of energy-efficient AI techniques, and full respect for circular economy principles and rules. This could include the set-up of specific schemes and criteria for conducting environmental impact assessments prior to the implementation of major digital transition projects, notably including those involving AI deployment.

R7. Enhance and enforce workers' rights in a digitally enabled workplace.

The digital transformation of many sectors/ ecosystems can lead to significant changes for European workers. The Covid-19 pandemic is already showing an acceleration of digitalisation, which risks leaving entire areas of the EU, and their respective workers, behind. While the pandemic triggered an enormous intensification of work for many EU workers, at the same time many companies have realised the benefits of working from home, increasingly cutting costs – often to the disadvantage of employees. The question of redistribution in terms of productivity gains through digitalisation is rarely talked about but reveals looming social inequality ramifications and also implications for intensified working conditions – which would run completely counter to the vision of Industry 5.0. The strong backlash against collective bargaining and social dialogue is also critical, particularly in some EU member states. As a result, trade unions are increasingly concerned about attacks on collective bargaining, the weakening of social dialogue and an intensification of work as a result of digitalisation.

In the context of the Recovery and Resilience Facility, and in line with the SDGs, it is essential to ensure that the whole European workforce benefits from the industrial transformation, and that workers' freedoms in both a physical and a digital working environment are guaranteed. Workers in less digitally connected countries should thus enjoy the same rights and opportunities. If not, societal and educational gaps will likely increase at the risk of jeopardising EU cohesion.

To avoid this scenario, the impact of AI and automated decision-making systems on workers should be monitored on an ongoing basis. The proposed AI Act would prohibit certain practices and introduce strict rules for high-risk AI used in recruitment and human resources. Companies should be required to disclose any data processing of their employees to the competent authorities.[7] Provisions for signing workforce surveillance practices or other forms of analytical assessment throughout recruitment or the entirety of employment should be prohibited.[8] Consent to the processing of worker-related data and to profiling based on machine learning should only be given collectively. Management should interact with trade unions or works councils, disclosing the data collected on workers, the algorithms used to process them, the data used to train them, the metrics used to evaluate work and the performance targets applied to workers. Workers should be able to detect errors or unfair treatment in this automated processing, report them and gain redress.

R8. Seize the opportunity and adopt 'AI for good' as a key policy priority.

AI-enabled solutions, properly deployed, have proved helpful in pursuing the common good, including the SDGs. This requires adherence to trustworthy AI principles and the availability of large amounts of data from both the public and private sector.

Common problems require shared solutions. It is therefore important to recognise and support the potential of AI from a public policy angle. As such, homes are becoming safer and more energy efficient due to smart home technology and services, and home automation, or domotics, is becoming a big part of the construction industry. **AI systems in urban contexts** are already integral to managing the transport systems of cities and supporting various urban systems and domains such as traffic, air quality monitoring, rubbish collection and energy. Through the lens of **smart and sustainable cities**, AI can support the use of digital technologies to make infrastructure services more efficient by operationalising smart urban transport systems via mobility-as-a-service (MaaS), which integrates various transport services into a single on-demand mobility service. As such, Helsinki was one of the first EU cities to implement MaaS, encouraging its citizens to replace private cars with a flexible transport subscription, embracing a sustainable lifestyle. AI-driven cars also support the gradual **transition to semi-autonomous transportation systems**. At the core of improving transportation systems is the capability of AI systems to reduce resource consumption, increasing environmental quality and cutting down on carbon emissions. All of these changes could gradually add up to a new, connected and more efficient system for EU cities and regions. This model – in the EU still more a glimpse into the future – is a reality in China and Malaysia, where so-called city brains (large-scale urban AI systems) manage the transport, energy and safety systems of several cities.

Besides transitioning to smart and energy-efficient city systems, the outstanding potential of AI to achieve **environmental sustainability**, in particular to meet the SDGs, is also applicable to land, water and biodiversity. As such, **clean water security** (water supply quantity, quality and efficiency management; water catchment control, sanitation and drought planning), **sea/ocean health** (sustainable fishing; pollution monitoring, reduction and prevention; habitat and species protection; and acidification reduction) and **weather/disaster resilience** are areas with great potential for AI to understand and improve the environment, combining machine-learning algorithms and climate models. AI applications are used for **cleaner air**, as seen with pollutant filtering and capture; pollution monitoring, reduction and prevention; early pollution and hazard warning; and clean energy production. Further, multiple-object detection AI for remote sensing with autonomous drones has been applied to **preserve biodiversity** (monitoring species and modelling their extinction; reducing and preventing pollution; controlling disease; and mapping complex impacts of co-dependent ecosystems) in the EU and worldwide.

In this context, the emerging AI PPP is directed at boosting the industrial uptake of AI and ensuring EU leadership in developing and deploying trustworthy AI in line with its fundamental rights. This ambitious and industry-driven AI strategy will need to be adequately designed to avoid creating an 'isolated ecosystem' or hampering market entry by imposing compliance costs that are too high. The AI strategy will have to be usefully combined with the data, edge/cloud and IoT strategy of the EU, focusing research and innovation on emerging areas such as 'embedded AI', thus combining hardware and software components to deliver outstanding performance improvements. Likewise, as the **AI value chain ranges from business transformation and systems development to legal and ethical issues**, innovation-friendly solutions to develop and test breakthrough technologies (deep AI), such as regulatory sandboxes and innovation schemes in those areas, are paramount to supporting the pursuit of AI as a force for good.

The forthcoming AI PPP, together with other initiatives on the edge/cloud and the IoT, as well as sectoral initiatives such as the Data Spaces, EIT Knowledge and Innovation Communities and Horizon Europe Missions and Partnerships, should work together to **create an environment that is conducive to the swift and inclusive application of AI techniques to address common challenges. These include climate change, infectious diseases, non-communicable diseases, biodiversity, agrifood sustainability, and the protection of democracy and fundamental rights**. The pursuit of AI as a force for good can also be a suitable terrain for future global cooperation on AI. As stated previously, this endeavour should remain consistent with the key principles of human centricity, resilience and sustainability, broadly interpreted.

3. THE EDGE/CLOUD LAYER, DATA SPACES AND THE FUTURE OF GAIA-X

R9. Complete the puzzle: EU data governance is still fragmented and uncoordinated.

The Working Group analysed the various elements that should contribute to the completion of the whole EU vision on the data economy. These include the data protection framework, including notably the GDPR; the need for personal information management systems such as IHAN or MyData, which implement user control over personally identifiable data; provisions on the creation of a market for non-personal data, such as the proposed Data Governance Act (DGA) and forthcoming Data Act; rules on trustworthy AI; the European Alliance for industrial data, cloud and edge; the governance of data spaces, currently defined in a non-homogeneous way; the nascent European Cloud Federation; and the European Interoperability Framework, with related initiatives such as eIDAS and the Single Digital Gateway. It is of utmost importance that all of these **policy and funding streams are made coherent, and that the various overlaps between them are resolved to ensure seamless data flows and the protection of user rights**. These policy streams should also be consistent with human-centric, resilient and sustainable technology features, as well as with the overall goals of the Green Deal. Only in this way will the twin transition fully take shape.

R10. Ensure a single market for IoT/edge applications and architectural solutions.

The Covid-19 pandemic has uncovered the many virtues of decentralised governance, including in industry and data transmission. In contrast to centralised cloud computing, edge computing allows for the real-time collection, analysis and use of data directly on devices (or close to them), rather than being transmitted to the central data server/cloud. Edge computing has become increasingly relevant because of higher volumes of data production, traffic, analysis and storage capacity. Limiting factors to an edge environment are bandwidth capacities (as discussed in R1-4) and security risks. The reference architecture model for edge computing (RAMEC) of the Edge Computing Consortium Europe (ECCE) reflects in its technical framework six cross-layer concerns and seven system/device hierarchy levels (i.e. the level of the 'edge' where the computing capability is located). This model highlights the current challenges and open issues in the field of edge computing, and shows that various layers and hierarchies make applied edge computing very use-case specific.

IoT and in particular **Industrial IoT (IIoT)** systems facilitate a range of processes in social, economic and environmental use cases. They can reduce costs and increase efficiency through predictive maintenance (manufacturing); enable home and mobile healthcare and connect patients with medical staff (healthcare); integrate sustainable energy sources in the power grid and reduce energy waste through improved energy load management (energy sector); and improve traffic systems through better resource management, eventually revolutionising transport through autonomous vehicles (mobility).[9] These examples are taken from Renda and Laurer's (2020) analysis of the potential of IoT systems, which the authors consider as essential enablers for achieving the **UN SDGs and the EU Green Deal**.[10] Depending on the use case, sector and level of autonomy/security, the IoT environment functions within a cloud and edge computing infrastructure. For instance, as shown in this agriculture case study, an IoT platform based on edge computing is used to monitor livestock and crops, as well as to manage farming resources in order to analyse profitability and environmental monitoring. This is advantageous as the deployer bears lower costs compared to a pay-per-use model for cloud services; it reduces the volume of traffic transferred between the IoT layer and the cloud; and machine-learning models can run at – or close to –

the devices, reducing response time and providing a certain level of service also in rural areas with low levels of connectivity. This is why edge computing has also been described as a **paradigm shift in the IoT**, as advanced novel architectures build on edge concepts, including fog computing, dew computing, multi-access edge computing (MEC, formerly mobile edge computing), the deep edge that encompasses distributed computing, advances in AI chips for inference and learning, distributed ledger technologies (DLT) and innovative sensing/actuating concepts. The EU Sustainability Roadmap for Edge Computing systemically considers certain sustainability factors in edge computing, including security and privacy issues; real-time, learning and 'smart' capabilities; management; and monitoring/ traceability considerations.

'Embedded AI' applications should therefore be actively promoted in the EU's digital and data-rich industrial ecosystems. Stronger efforts should be directed towards capitalising on the EU's edge/IoT computing leadership to leverage opportunities from enhanced data and software exchange for edge computing. Specifically, the EU industrial strategy should **prioritise solutions that leverage decentralised data analytics architectures** to foster cost-efficient, resilient and sustainable solutions. Until now, the EU institutions have not given sufficient attention to the blossoming world of the IoT, which presents enormous opportunities, but also massive security risks. The work on trustworthy AI should also become a reference for developing criteria for trustworthy IoT, solutions, in particular concerning fundamental rights and socio-technical robustness, which often lack adequate safeguards in the emerging IoT market.[11]

R11. Ensure that GAIA-X is scaled up into the European Alliance for industrial data, cloud and edge.

One of the Commission's key aims is to ensure that EU citizens and businesses fully reap the benefits of the EU's data, and that requests from third countries to access non-personal data are refused. This is seen as a means to assert data sovereignty in Europe in a global context where the EU can gain value from its industrial data. GAIA-X is the associated non-profit association (European Association for Data and Cloud) with 22 EU founding members and over 200 international membership applications. Its ambitious objective is to operationalise transparency and interoperability in a new, Europe-wide business network composed of a range of data ecosystem providers, including cloud solution providers (CSPs), high performance computing (HPC) and sector-specific cloud and edge systems.

The GAIA-X infrastructure is composed of three interdependent layers: (1) data ecosystems (ensuring data space and application programming interface (API) interoperability to foster e.g. common AI, IoT technologies or big data marketplaces and applications in/across sectors); (2) infrastructure ecosystems (aligning network and interconnection providers, CSPs, HPC and sector-specific cloud and edge systems to identify and connect participating providers and services); and (3) federation services (identifying the minimum technical requirements and services necessary to operate the federated GAIA-X ecosystem for providers, based on EU values and principles). In parallel, the European Alliance for industrial data, cloud and edge aims to bring together member states, cloud providers, cloud users from different sectors, and stakeholders from academia and civil society. In order to build up a European cloud and edge service that is trustworthy, energy efficient and competitive, interoperability and open source standards are key to allowing multi-vendor interactions on these cloud/edge platforms.

It is essential to **step up the coordination of two overarching EU instruments: GAIA-X and the European Alliance for industrial data, cloud and edge**. This is necessary for the economic and social sustainability of EU industrial ecosystems. So far, the digital transformation has led a subset of players, mostly at the platform layer, to harvest the value of the vast amounts of EU-generated data, also given that the storage, processing and monetisation of these data happens elsewhere. To redistribute this value and ensure that the EU economy and its citizens benefit from it, **the current EU data economy needs to be characterised by interoperability, openness and transparency**. In this respect, GAIA-X could become the blueprint for setting up common European data spaces, but only if the latter are coherently linked to the mechanisms in the Alliance.

The EU cloud rulebook, including, standards, reference architectures, use cases and data spaces, should also be an integral part of GAIA-X.

R12. Establish a 'compliance by design' mechanism with EU legislation for members joining GAIA-X.

GAIA-X is a federated infrastructure ecosystem connecting participating EU and non-EU businesses, regardless of size and data capacity. Important principles for upholding EU values include security and privacy 'by design', transparency and respect for data rights. In the interest of guaranteeing a European direction and destiny for the project, German Economy Minister Peter Altmaier argued that a cloud infrastructure administered by the EU could restore its "digital sovereignty and counter unfair competition from state-controlled and state-subsidised companies from third countries (read China) and by market dominant online platforms (read US)". In order to achieve this, however, it is essential to compile a clearly defined and enforceable rulebook for all, especially non-EU companies.

The GAIA-X rulebook should ensure that EU fundamental rights and values are protected, while industrial capacity in critical digital infrastructure is enhanced. Therefore, the rulebook for new members and entities joining GAIA-X should translate EU principles and values into actionable processes and checks for technical practitioners. This includes detailed provisions on data transfers, open data, data integrity/consent and opt-out models for consumers, minimum requirements for datasets, cybersecurity provisions, and more guidance on compliance with EU technology regulations such as the GDPR or the proposed regulation on AI. Compliance with EU policy and its principles of privacy, trust and transparency by design would also benefit regulatory authorities and market surveillance.

R13. Step up the ambition of the Data Governance Act.

Common European data spaces are infrastructures designed to create data-sharing platforms: their main leverage will be the possibility to reuse data. The DGA will define an open ecosystem, independent of big players, in which greater involvement leads to increased value. Key components are: (1) facilitating the reuse of **data created or held by the public sector**; (2) creating **trustworthy data providers**; and (3) operationalising the concept of **data altruism** through the creation of a registry of voluntary entities, making their collected and processed data available for altruistic purposes. In so doing, the DGA challenges the dominance of Big Tech over personal data brokering by empowering consumers and unlocking new business opportunities for EU start-ups and small and medium-sized enterprises (SMEs).

With the creation of **European data spaces**, public and privately held data from across the EU can be exchanged securely and at a lower cost in an effort to boost the development of new data-driven products and services. These data spaces are targeting the following sectors: agriculture, energy, environment, finance, health, manufacturing, mobility, public administration and skills. The **environment data space** will be one of the first to be created and is envisaged to be a common data ecosystem to help e.g. cities achieve their climate goals through digital technologies. This is an urgent objective, but likewise a race against time, given the EU's commitment to a climate-neutral continent by 2050 and the objectives set out in the **EU Green Deal**, not least because large data centres consume considerable amounts of energy. The impact of digitalisation, together with the need to capture, transfer and process an increasing amount of data, will inevitably require new policy instruments to reach the 2030 and 2050 climate targets, according to a Commission-led study.

The ambition to create a common EU pool of data and in particular the nine data spaces mentioned above requires better guidance and links between regional, national and European entities alike. For instance, the health data space requires more stakeholder interaction and feedback in order to reap its full potential for practitioners and patients alike. Stakeholders and SMEs in particular need **clearer guidance about the roles of the European Data Innovation Board and the Support Centre for Data Sharing** in order to adapt their operations to the upcoming legislation.

Furthermore, as the current version of the DGA does not cover objects and devices connected to IoT environments, the industrial strategy should provide this crucial link by providing **incentives for actors and entities that generate value based on interconnected data-sharing services in the IoT environment**, through both edge and cloud computing, to support the uptake of high-value data sharing in the IoT.

More generally, there is a strong need to clarify the future patterns of **interaction between the new institutions foreseen in the DGA and other competent authorities**, either existing or those proposed by other EU legislative initiatives (Data Innovation Board, European Board for Digital Services, AI Board, European Data Protection Board and European Data Protection Supervisor). Synergies and overlaps should be thoroughly mapped so that SMEs and other businesses can adapt their operations to the relevant EU legislation. The same can be said for national competent authorities, which also feature a variety of possible overlaps.

R14. Foster interoperability as the key enabler of the EU's digital ambitions.

The DGA further aims to foster the availability and transmission of data by increasing trust in data intermediaries and strengthening data-sharing mechanisms across the EU. A key element of the DGA is to establish **principles for data sharing** between public and private sector entities. This new method of data governance is intended to increase trust in data sharing, particularly for data subjects (citizens), while making data more available from a technical viewpoint for its use and re-use for certain limited purposes.

Limited interoperability is one of the key issues cutting across policy areas, however, and one that is particularly relevant to the development of the common European data spaces. Enhanced interoperability is therefore necessary both at the technical and semantic level (i.e. common infrastructure and data models) and at the organisational and legal level (ensuring that processes within organisations and legal requirements do not hinder the exchange of data) in the development of the nine future data spaces, notably health and public administration. This includes the successful integration of personal and industrial, vertical, horizontal and diagonal data spaces.

The EU should foster the uptake of common standards for data in both the public and private sector, based on specific sectoral needs. This is essential to support data sharing, while ensuring that the overarching framework of the data spaces is underpinned by key principles such as trust, data protection and privacy. The role of trusted data intermediaries is particularly relevant, and the EU industrial strategy should actively foster the creation of data intermediaries and reward their efforts. In addition, best practices (e.g. on quality assurance and internal auditing processes) should be collected and published by the EU institutions to promote the uptake of data-driven operations. Making this data-sharing space as open and inclusive as possible is paramount to its success, and to advancing the European vision of a trusted space that protects democratic values, privacy and equality.

R15. Link data spaces to ecosystems.

Based on two key concepts in the European market – transparency and fair competition – the Open Data Directive will provide a common legal framework for government-held data (public sector information). Implemented at the national level, the Directive – a revision of the Public Sector Information Directive – aims to: (1) advance the publication of dynamic and real-time data and the uptake of APIs; (2) reduce the burden and costs for public bodies of data dissemination and re-use; (3) include data held by public undertakings; and (4) strengthen transparency requirements for all parties involved. This could facilitate the uptake of business ecosystems in the EU industrial strategy.

A key component will be the introduction **of high-value datasets**, expected to bring important benefits to society and the economy. These datasets should be available free of charge and for bulk download, supplied in machine-readable formats and APIs. This is a notable opportunity for EU researchers and businesses to gain significant insights, especially considering the interdependency of the datasets with the development of AI and other key computing techniques. The thematic categories of high-value datasets, as referred to in Article 13(1) of the Open Data Directive, are "geospatial, earth observation and environment, meteorological, statistics, companies and company ownership as well as mobility".

However, there is currently a disconnect between the aggregation of economic activities into (nine) data spaces, and the identification of ecosystems as the basic unit of analysis for the EU industrial strategy. To the extent possible, **the two concepts should be reconciled and coordinated**, so that the EU industrial strategy becomes more streamlined and easier to govern.

REFERENCES

Blackman, C. and S. Forge (2019), "5G Deployment: State of Play in Europe, USA and Asia", Study for the Committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

Body of European Regulators for Electronic Communications (BEREC) (2020), "Guide to the BEREC 5G Radar", BoR (20) 223, December.

Daly et al. (2020), "5G action plan review for Europe Report for Ericsson and Qualcomm", Analysis Mason, 23 September (www.ericsson.com/4ab850/assets/local/about-ericsson/company-facts/europe/5g-action-plan-review-for-europe-executive-summary.pdf).

European Commission (2021), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussels, 9.3.2021.

Forge S. and K. Vu (2020), "Forming a 5G strategy for developing countries: A note for policymakers", *Telecommunications Policy*, Elsevier, Vol. 44, No. 7.

GSMA (2019), "The Enablement Effect: The impact of mobile communications technologies on carbon emission reductions", December (www.gsma.com/betterfuture/wp-content/uploads/2019/12/GSMA_Enablement_Effect.pdf).

GSMA (2020), "5G and Data Privacy: An overview for policymakers", July (www.gsma.com/publicpolicy/wp-content/uploads/2020/07/GSMA_5G_and_Data_Privacy_July_20.pdf).

Hayes, J. (2020), "Network - Communication. 6G and the reinvention of mobile", *Engineering & Technology*, Vol. 15, No. 1, 11 February.

International Commission on Non-Ionizing Radiation Protection (ICNIRP) (2010), "ICNIRP Guidelines for limiting exposure to time-varying electric and magnetic fields (1 HZ – 100 KHZ)", *Health Physics*, Vol. 99, No. 6, pp. 818-836.

Moazzamipeiro, M. (2020), "5G Implementation: Major Issues and Challenges", Conference Paper for the 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran.

NIS Cooperation Group (2019), "EU coordinated risk assessment of the cybersecurity of 5G networks report", 9 October.

NTT DOCOMO (2020), "White Paper 5G Evolution and 6G", January (www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_20200124.pdf).

Oertel, J. (2020), "China: Trust, 5G, and the coronavirus factor" in C. Hobbs (ed.), *Europe's digital sovereignty: From rulemaking to superpower in the age of US-China rivalry*, European Council on Foreign Relations, July (https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/).

Saad, A. et al. (2020), "6G technology-based advanced virtual multi-purpose embedding algorithm to solve far-reaching network effects", *Computer Communications*, Vol. 160, 1 July, pp. 749-758.

Scientific Committee on Health, Environmental and Emerging Risks (SCHEER) (2018), Statement on emerging health and environmental issues, 20 December (https://ec.europa.eu/health/sites/health/files/scientific_committees/scheer/docs/scheer_s_002.pdf).

Theodosopoulos, V. (2020), "Looking beyond 5G: Why Europe is far from naïve when it comes to issues of strategic dependence", London School of Economics (LSE) Blog, July (https://blogs.lse.ac.uk/europpblog/2020/07/20/looking-beyond-5g-why-europe-is-far-from-naive-when-it-comes-to-issues-of-strategic-dependence/).

Thompson, L. and W. Vande Stadt (2017), "5G is Not the Answer for Rural Broadband", Broadband Communities, March/April (www.bbcmag.com/rural-broadband/5g-is-not-the-answer-for-rural-broadband).

Webb, W. (2019), *The 5G Myth*, Walter de Gruyter Inc., Deutsche Nationalbibliografie: Boston/Berlin.

LIST OF RECOMMENDATIONS

WORKING GROUP SESSIONS AND SPEAKERS

Co-Chairs: Andrea Renda, and Lorenzo Pupillo

Rapporteurs: Rosanna Fanni and Carolina Polito

ENSURING A SPEEDY, BALANCED ROLLOUT OF CONNECTIVITY TECHNOLOGIES

- Simon Forge, Director, SCF Associates

ARTIFICIAL INTELLIGENCE AND INDUSTRIAL TRANSFORMATION

- Lars De Nul, European Commission
- Sebastian Wieczorek, SAP
- Max Lemke, European Commission
- Judith Kirton-Darling, Deputy General Secretary industriALL
- Barry O'Sullivan, Professor, University College Cork

THE EDGE/CLOUD LAYER, DATA SPACES AND THE FUTURE OF GAIA-X: ANATOMY OF SINGLE MARKET 2.0

- Andrea Renda, Senior Research Fellow, CEPS
- Klaus Ottradovetz, Distinguished Expert Cloud, IoT, Blockchain, Atos.
- Jaana Sinipuro, Project Director responsible for the IHAN®, Sitra
- Jakob Greiner, Head of EU Regulatory Affairs, Deutsche Telekom
- Monique Calisti, CEO Martel Innovate and Digital for Planet

WORKING GROUP MEMBERS

The Working Group Members are comprised of representatives of commercial companies, trade associations, consumer interest groups and individuals from EU Institutions, policymakers, academics, regulators and supervisors. They are participating in the activities of the Task Force in a personal capacity.

CORPORATE MEMBERS

- Afore Consulting
- American Chamber of Commerce to the EU (AmCham EU)
- Apple
- Association française des entreprises privées (AFEP)
- Assonime
- BNP Paribas Fortis
- Cassa Depositi e Prestiti
- Danish Agriculture and Food Council (Agridan)
- Deloitte
- Deutsche Telekom AG
- Électricité de France (EDF)
- European Federation of Pharmaceutical Industries and Associations (EFPIA)
- European Wireless Infrastructure Association (EWIA)
- Facebook
- FTI Consulting
- Huawei
- Intesa Sanpaolo
- JPS Public Policy
- Martel Innovate
- McKinsey & Compay
- Microsoft
- MSD/Merck
- Muzinich & Co.
- Orange
- Phoenix Tower Interntaional
- Saher EU
- Samsung Electronics
- SCF Associates Ltd
- Siemens
- Telefonica SA
- Uber
- Wavestone

INSTITUTIONAL MEMBERS

- Eurofound
- European Bank for Reconstruction and Development (EBRD)
- European Commission
- European Committee of the Regions (CoR)
- European Bank for Reconstruction and Development (EBRD)
- European Defence Agency (EDA)
- European Free Trade Association (EFTA)
- European Investment Bank (EIB)
- European Investment Fund
- European Parliament
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Italian Innovation Fund
- Organisation for Economic Co-operation and Development (OECD)
- United Nations Industrial Development Organization (UNIDO)

CIVIL SOCIETY AND ACADEMIA

- AI Governance International
- AllBe
- Bellona Europa Org.Internat
- Brookings Institution
- Centre national de la recherche scientifique (CNRS)
- Chalmers University
- College of Europe
- ecoSurge
- Foundation for European Progressive Studies (FEPS)
- Georgia Institute of Technology
- German Marshall Fund
- Hertie School
- Humanity of Things
- IHAN – Human-driven data economy
- industriAll European Trade Union
- LUISS University
- Mercator Institute for China Studies, MERICS (gGmbH)
- Sciences Po
- University of Ferrara
- University of Namur
- University of Pavia

AUTHORS

Andrea RENDA is Part-Time Professor at the School of Transnational Governance of the European University Institute, in Florence (Italy). He is a Senior Research Fellow and Head of the CEPS Unit on Global Governance, Regulation, Innovation and the Digital Economy (GRID). Andrea is also a non-resident Senior Fellow at Duke University's Kenan Institute of Ethics and he was Adjunct Professor of Law and Economics at Duke Law School (United States) for Academic Year 2016/2017. He is also Visiting Professor of Competition Policy and the Digital Economy at the College of Europe in Bruges (Belgium). He is also a Fellow of the World Academy of Arts and Science, and a CITI Fellow at Columbia University's Centre for Tele-Information. He is a member of the EU High Level Expert Group on Artificial Intelligence; a member of advisory group on Economic and Societal Impacts of Research (ESIR), for the European Commission, DG Research and Innovation; and since October 2020, a member of the European Parliament's STOA international Advisory Board. His current research interests include regulation and policy evaluation, regulatory governance, innovation and competition policies, and the ethical and policy challenges of emerging digital technologies, in particular Artificial Intelligence. A very prolific author and keynote speaker, Andrea provides regular advice to several institutions, including the European Commission, the European Parliament, the OECD, the World Bank, the Inter-American Development Bank, and many more.

Lorenzo PUPILLO is an Associate Senior Research Fellow and Head of the Cybersecurity @CEPS Initiative. Before joining CEPS, he served as an Executive Director in the Public & Regulatory Affairs Unit of Telecom Italia developing the company' global public policies for Internet, Cyber-Security, Next Generation Networks. He also managed Telecom Italia's relations with the OECD, the ITU and other international associations and organizations. Previously, Dr. Pupillo held a variety of senior positions in the Strategy, Business Development and Learning Services divisions of Telecom Italia. He is an economist by training and has worked in many areas of telecommunications demand and regulatory analysis, publishing four books on Internet Policy and many papers in applied econometrics and industrial organization. He has served as an advisor to the Global Information and Communication Technologies Department of the World Bank. Before joining Telecom Italia, he was member of the technical staff at AT&T Bell Laboratories in Murray Hill – New Jersey – and he worked as senior economist for governmental institutions. Dr. Pupillo is also an affiliated researcher at Columbia Institute for Tele Information at Columbia Business School and serves on numerous scientific and advisory boards around the globe. He obtained a Ph.D. and an M.A. from University of Pennsylvania, an MBA from Istituto Adriano Olivetti in Ancona Italy and an MS in Mathematics from University of Rome.

Rosanna FANNI is associate research assistant and Digital Forum coordinator at CEPS in the GRID Unit. She currently investigates the impact of AI on fundamental rights in the EU. She also analyses the implications of the EU's digital strategy on transatlantic relations and will be a Fulbright visiting researcher at the Brookings Institute (Washington DC) in 2021. Rosanna recently graduated from the Erasmus Mundus MA in Digital Communication Leadership, specialising in policy and innovation in the EU.

Carolina POLITO is research assistant at CEPS in the GRID Unit, more specifically in the Cybersecurity@CEPS Program. Her main expertise is in the field of cybersecurity and Internet governance, acquired through different work experiences in European and non-European research institutes over the past two years. She holds a Master's Degree cum Laude and a Bachelor's Degree cum Laude in International Relations from the University of Bologna.

NOTES

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussels, 9.3.2021 (https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf).

[2] According to the definition provided in the EU Digital Compass, "an edge node is a computer that acts as an end user portal (or 'gateway') for communication with other nodes in cluster computing, where components of a software system are shared among multiple computers". European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussels, 9.3.2021.

[3] Some members of the Task Force disagree with this point.

[4] This section was contributed by Jean Paul Simon, JPS Public Policy Consulting. We wish to thank him for his input and the knowledge that he brought to the CEPS Task Force.

[5] Some members of the Task Force disagree with this statement. In these participants' view, for rural areas a mix of technology might instead be promoted, relying on fibre, 5G, 5G fixed wireless access (FWA) and others such as satellite.

[6] Some members of the Task Force disagree with this point.

[7] Pursuant to Article 9 GDPR, which specifically prohibits the processing of "special categories of personal data" that explicitly describe the current situation of a person, such as health, trade union membership, ethnic origin, religious/philosophical belief, sexual orientation, genetic data and biometric data for the purpose of identifying an individual, it should be specified that the prohibition of data also applies to machine-learning systems that predict or implicitly evaluate this information using indirect data sources.

[8] This is necessary as the prevailing power structures in employment or dependent work contexts threaten individual and freely given consent (GDPR, Art. 4(11)).

[11] Laurer and Renda (2020).