Axel Voss
Member of the European Parliament

A manifesto for Europe's digital sovereignty and geo-political competitiveness

The digital transformation continues to have a strong impact on our day-to-day life and has led to radical changes in almost every part of Europe's economy and society. Although the EU Digital Single Market strategy was a first important step to make the European Union future-proof for the digital era, I believe that many relevant policy questions remain unanswered.

Despite our ambition to remain competitive at the global level, we are falling more and more behind in the digital world. In 2019, none of the top fifteen digital companies is European. There is no significant European (computer or mobile) operating system, browser, social media network, messaging service or search engine to speak of. While there are European system integrators, telecom providers or network manufactures that are still global leaders, our growing dependence on foreign software, hardware and cloud services is deeply worrying. Given how strongly the digital transformation is currently driven by these three sectors as well as by leading digital platforms, there is a strong risk that the next decisive technological stage may be entirely shaped by non-European actors, which often do not share our core values, traditions and standards or even try to undermine them. The potential consequences in terms of prosperity, privacy and security cannot be underestimated. Nonetheless, our response to this challenge has so far been a wide range of incoherent, fragmented interim solutions following lengthy decision-making processes. Not only will this approach prevent us from ever catching up with a rapidly changing technological environment – it may also give our citizens the impression that the European political class has lost control – a perception that could ultimately result in a significant loss of trust in our democratic system.

This scenario urgently calls for a comprehensive, consistent and horizontal digital policy agenda. At its heart should be the concept of 'digital sovereignty' – a European way of digitization, which contrasts with the US-American or Chinese approach and is human-centered, value-oriented and based on the concept of the social market economy[1]. It would create a digital environment for individual self-determination and legally guaranteed personal freedom, while at the same time reducing our dependency on foreign hardware, software and services.
However, striving for 'digital sovereignty' does not mean that the European Union should become protectionist. We are and should always be a champion of international cooperation, free data flow and trade. We also have to acknowledge that many digital innovations rely on complex value chains, collaborative ecosystems and well-functioning relations with our international partners. Therefore, 'digital sovereignty' should rather mean that we increase our ability to take independent decisions on the parameters we want to use for digital technologies. Instead of excluding all non-European companies from the Digital Single Market, we should even increase the cooperation with our trustworthy international partners that share our values. At the same time, we should make decisive long-term investments in key sectors to give us more options to choose from and to enable European businesses to compete and grow - both across the EU and in the global market.

Implementing this agenda will not be easy and requires, inter alia, the introduction of new ideas and concepts into the political debate, closer cooperation with the private sector as well as civil society, a better balance between innovation and regulation and, crucially, legislative procedures that can keep up

[1] A socio-economic model that combines a free market economic system with specific social policies. The goal is to ensure fair competition within the market as well as a maintaining functioning welfare state.

with the fast pace of digital transformation. Prior to this, a thorough strategic analysis is needed. We need to have a clear picture about our areas of strength that we should reinforce, our critical deficiencies that we should overcome and the upcoming disruptive technologies in which strong investments make sense. Being convinced that this approach is Europe's best option for a prospering digital future, I call on all EU institutions to commit to a **Digital Single Market 2.0**.

Over the last months, I have widely consulted on the subject with citizens, academia, consumer organizations, social partners, NGOs, the private sector, judges and parliamentarians as well as European agencies and national ministries. Together, we have identified a comprehensive range of challenges and solutions, which are listed in the annex to this manifesto. I profoundly support this agenda and will dedicate my mandate during this legislative term to contributing to its realization.

<u>The key components of this new digital agenda are:</u>

- Europe needs to achieve **digital sovereignty** by introducing a 'European way' towards an increasingly digitized world, in particular by developing a strategic digital agenda that includes large investments as well as close cooperation with the private sector in a range of digital flagship areas. Our objective should be to become less dependent on non-European technologies and services, while establishing sound ethical, technological and security standards for those that we cannot produce ourselves or where purchasing makes more sense for the time being. Sensitive digital technologies should only be procured from trustworthy international partners and cooperation should exclusively take place with partners that share our values or at least respect them.

- Europe needs to advance the **Digital Single Market** by updating its competition policy, by pushing for a fair and effective taxation system for digital companies, by improving our digital infrastructure, by increasing our cyber security resilience and by facilitating investment as well as access to public funding. Our objective should be to prevent abuses of market power in the digital economy more effectively and to better enable European companies to scale up. Moreover, we should strive to introduce a 'Digitized in the EU' brand that is based on our high ethical and data protection standards and which offers our citizens (and consumers from outside the EU) digital products and services they can genuinely trust.

- Europe needs to change the way its **political processes and governmental systems** work by making legislative procedures more effective, by introducing e-governance services on a large scale and by better safeguarding our citizens and democratic systems. Our objective should be to adopt principle-based and tech-neutral legislation while making our political system more resilient against cyber-attacks and our political responses more effective in a rapidly changing digital world. Regular impact assessments and immediate adjustments to new developments should become a default feature in all areas.

- Europe needs to ensure that the **digital life of our citizens** is based on a fair, safe and sustainable foundation by avoiding gaps in digital connectivity, by improving digital literacy, skills and critical thinking about the use of new digital tools, by promoting sustainable digital technologies and by establishing legal frameworks that prevent data or consumer protection violations. Our overall objective should be to find the right balance between the necessary protective measures on the one hand, while on the other hand providing our citizens, businesses and universities with the space to enjoy their digital freedom, to grow their business or to innovate.

ANNEX

A. POLITICS

The age of digital geopolitics: Without any own vision and long-term strategies, Europe has so far been a bystander in the battle for digital supremacy between China (authoritarian and state-controlled economy) and the USA (disruptive innovation by dominating tech corporations). While both countries are quickly evolving to the new circumstances in the digital world, Europe often passively observes their progress. As a result, our dependence on foreign technologies is constantly growing.

- Encourage and lead international efforts towards a global Digital Convention, providing a comprehensive international legal framework for the new challenges of digitalization, foreseeing accountability mechanisms, while reinforcing the link to international human rights standards.
- Develop - in close cooperation with all relevant stakeholders - a digital agenda that introduces a 'European Way' as an alternative approach in the digital world. While promoting European key sectors and safeguarding critical infrastructures, this agenda should also be human-centric, inclusive and in line with the EU Charter of Fundamental Rights. However, we should also carefully consider and identify where it is not reasonable from an economic, budgetary or security point of view to make large investments to build up our own capacities. In those cases, Europe should continue to draw on foreign technologies and services from trustworthy partners by establishing clear legal requirements which standards have to be fulfilled and which security concerns have to be met.
- Introduce a legal framework and a comprehensive plan on how to increase Europe's strategic digital autonomy by determining flagship areas (e.g. Artificial Intelligence, quantum computing, Distributed Ledger Technology, robotics, biotech). The framework should be the starting point of a long-term process with regular evaluation. In particular, we need to foster research and development of components to achieve strategic independence from foreign suppliers. The European Union shall closely cooperate with existing business alliances and multi-stakeholder initiatives that already aim to democratize and diversify crucial Internet infrastructure (physical and virtual). It shall facilitate the creation of cross-border networks, including through targeted funding.
- Introduce a 'Digitized in the EU' brand based on Europe's high ethical and data protection standards. Digital products and services carrying this label would offer consumers a local and trustworthy alternative. At the same time, it could give our private sector a unique competitive edge on global markets by providing a level of trust unmatched by any other region. To make this concept work, we need to define clear criteria for this label (e.g. whether all, a majority or certain parts have to be of European geographical origin in order to qualify).
- Conduct a study that explores and identifies the benefits of a free-market approach compared to state intervention to advance the new digital agenda. The objective is to deliver conclusions on Europe's best options to adapt to the new realities and global challenges of the digital transformation while safeguarding our established values and traditions.

Legislative procedures: The traditional ways of law-making have proven to be too static and too slow in order to respond adequately to a constantly changing digital world.

- Ensure – where possible – principle-based, technologically neutral and, above all, future-proof legislation for the fast-paced digital economy and quickly emerging technologies.
- Complement our legislative procedures with new approaches for digital issues that are able to deliver quick and effective solutions by adopting and implementing legislation after a few months instead of years, whilst respecting fundamental EU law-making principles such as transparency, the rule of law and proportionality. Implementation should always include parallel impact assessments that are based on market economic analysis. The results of those assessments should be regularly reviewed in order to immediately fix political misjudgments

with legal adjustments. A 'rapid reaction committee' on digital issues with standing rapporteurs should be in charge of these new legislative processes.

- Call on the European Commission to only propose regulations and use full harmonization for all digital matters as the DSM 2.0 needs to be genuinely harmonized. Many files of the past legislative period (e.g. copyright directive, digital content directive, Audiovisual Media Services directive) will lead to 27 different national laws as well as different legal interpretations[2] although they are based on the same set of rules. This is a situation we cannot allow any longer, in particular as the digital sphere is characterized by rapid cross-border dynamics.
- Examine how the EU policy-making process can be improved. I would suggest the following:

  a) Conduct more rigorous impact assessments before the proposal is submitted to the European Parliament and the Council. The amendments brought forward by Parliament and Council should also be reviewed with impact assessments;

  b) Foster closer cooperation between European Institutions and stakeholders, in particular by exchanging information / best practices systematically to ensure that the legislative files are balanced and implementable;

  c) Create a digital scrutiny reserve that examines if the proposed legislation contradicts Europe's digital objectives and improves our competitiveness. Such an approach would ensure coherence between different files;

  d) Use regulatory sandboxes for innovative businesses to help them become compliant.
- Use modern ways of communicating with citizens - especially with the younger generation: the European Institutions should develop new media concepts and strongly cooperate with private actors to this end. The aim should be to invest 40% of the PR-budget as a minimum in online communication, in particular social media channels.

Electoral integrity: Today's digital environment makes it very easy for European and non-European actors to influence voters or even manipulate entire elections, which is threatening a central pillar of our democratic systems.

- Complement the voluntary measures to fight political disinformation and to protect the integrity of elections in the 'Code of Practice on Disinformation' with legislation. The goal should be a reliable shutdown of bot-nets as well as fake accounts and the complete stop of payments (advertisement revenues) to account holders that spread political disinformation. To this end, all relevant stakeholders should be consulted and best practices should be shared among all platforms.
- Encourage Member States to develop digital voting systems to make elections more accessible, auditable, efficient, secure and transparent, while providing analogue voting options and preserving analogue voting result backups. Assess whether the combination of state election systems with specialized encrypted platforms is a way to improve electoral integrity and security[3].

B. SECURITY

Cyber security: Despite important legal achievements during the previous legislative period, the damage caused by cyber-attacks on our citizens, businesses and institutions is increasing.

[2] This situation is even worse in federal states with different regional authorities.

[3] Internet companies have developed the following system: when the electorate cast their votes, it receives a tracking code and the data enters both the traditional and the digital platform. In parallel, the normal state-run tabulation process and the platform then record all votes and tabulate them. In the end, the results of both calculations could be compared in order to exclude machine errors, hacks or manipulations.

ANNEX

- Full implementation of existing legislation in all Member States, in particular the 'Cyber Security Act', the 'Network Information Systems' (NIS) Directive, and the directive for the protection of trade secrets. Use the upcoming NIS-review to transform it into a directly applicable regulation, to broaden its scope to include more sectors and to assess if there are any duplications in light of existing GDPR obligations. Overall, one should guarantee that all cyber security measures by the European and national legislators are coherent and do not become a competitive disadvantage.
- Cooperate closely with the private sector to develop schemes based on the 'Cyber Security Act' and other relevant legislative initiatives in order to make them relevant to the market and keep them up-to-date with the pace of technological change as well as the evolution of threats. With regard to the current debate on the security and trustworthiness of 5G networks, a European scheme for 5G network components is of utmost importance and urgency. The EU needs to ensure that hard- and software components utilized to build the European 5G network are as cyber-resilient as possible.
- Establish a list of risk-based mandatory cyber security requirements that all products and services have to meet. However, it should be based on the associated risk in the specific sector and the degree of influence on the risk in order to avoid disproportionate burdens for SMEs and start-ups. A sector specific approach under the supervision of ENISA seems therefore reasonable. Last but not least, the list should cover the entire lifecycle of a product from development (e.g. code testing and verification) to maintenance (e.g. patching and updates) until the end of its lifetime. It has to be clear that each company in the supply chain has to play its role in contributing to the creation of resilient products and services.
- Encourage every European and non-European enterprise that is active in the Digital Single Market to develop a clear and regularly independently evaluated cyber security strategy, based on its individual risk situation. To avoid additional red tape, the EU could support this process by establishing a common platform that shares best practice examples, announces the latest vulnerabilities and provides legal advice. Encourage and financially enable ENISA and national agencies to constantly analyze the threat level in every relevant sector and to publish sector-specific recommendations.
- Cooperate with Member States to promote the establishment of mandatory cyber security trainings for the workforce[4] on a large scale throughout the European Union to raise awareness and to minimize risks related to the human factor in cyber security.

Cyber defense: the modern conflict landscape is characterized by an increasing amount of hybrid elements with cyber attacks being among the most frequent. In the absence of a clear strategy, attacks by organized crime, terrorists or state actors often remain unanswered.

- Cooperate with NATO, the G20 and OECD against non-cooperative third countries from which cyber-attacks originate in order to enable diplomatic reactions and economic countermeasures. Consider the termination of EU financial aid against countries that do not cooperate, do not share information or do not prosecute cyber-attack related activities.
- Explore the creation of cyber defense related military structures in the context of PESCO. Moreover, establish a 'European Cyber Security Response Force' to enhance capacities for quick reaction in case of cyber-attacks, in particular on critical infrastructure. The objective would be to give the EU clear procedures for a coordinated and quick reaction to cyber-attacks, covering measures in the political, economic, diplomatic and military domain.
- Introduce legislation to make cyber resilience and recovery mechanisms mandatory for critical infrastructure. This should cover both technical as well as organizational measures such as fire drills. In addition, improve resilience against data-based, psychological attacks on political opinion-forming processes and elections.

[4] Not only employees but all citizens should participate in cyber security trainings as consumers of a digital product or service are often the biggest security risk. See also F) Society: 'Employment, education and digital skills'.

- Conduct a study on additional legislative measures for the EU to counter cyber-attacks that are financed and organized by third countries, while using existing technologies more efficiently (e.g. security/privacy by design, encryption, quantum computing). Create a permanent multi-sectoral and multi-stakeholder working group to observe the latest developments and propose necessary adjustments. The research and the development for improving capabilities to address cyber threats should be a priority of the European Defence Fund.

Digital Criminal Justice and Law Enforcement: our police forces and judicial systems are not able to keep pace with criminal individuals or groups and terrorists who act and cooperate more and more globally while using expensive and state-of-the-art technologies.

- Accelerate the efforts of all EU institutions to reach an agreement on e-evidence, which includes legal remedy mechanisms in case of law enforcement requests that are not in line with the respective national law. Establish a fast, reliable, secure and interoperable infrastructure for the exchange of data between national police and the judiciary as well as all justice and home affairs agencies. A secure platform that enables companies to share their data in response to a data request from a foreign authority would lead to better traceability of the requests and data movements.
- Enter into negotiations for an international executive agreement between the EU and the US in order to address conflicts of law and to set up common rules for obtaining electronic evidence. Use the e-evidence proposals as a basis for negotiations and introduce corresponding safeguards in the agreement (e.g. criminal procedural law rights, data protection, security and transparency obligations in line with EU-legislation).
- Participate actively in the negotiations on the 2nd Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) to ensure the compatibility of its provisions with EU law as well as Member State obligations deriving from it.
- Establish an encrypted channel that allows European and national entities to communicate safely with each other, redesign the EU-wide case management system and make the 'European Judicial Counter Terrorism Register' operational across Europe during the next months. Update the EU-architecture for law enforcement cooperation based on the Prüm Convention by creating a genuinely interconnected network of law enforcement authorities with EU agencies at the center.
- Ensure that the entire security chain receives adequate funding via the Multiannual Financial Framework, as an effective judicial system is needed to successfully conclude the results of criminal investigations by law enforcement forces.
- Conduct a study about the compatibility of digital surveillance (use of backdoors in encrypted communication, seizing virtual assets and of data retention) with European law, fundamental rights as well as the established legal practice of the ECJ.

C. COMPETITION

Market conditions: the Digital Single Market is dominated by powerful non-European players. This means European companies face structural disadvantages when trying to catch up technologically and to reach the scale and strength needed to compete at European and global level. While the completion of the DSM is a key prerequisite to create a strong home market for European companies, active competition policy and enforcement should also become a priority.

- Reform the current national and European competition and antitrust framework to better target abuses of market power in the digital economy as well as to address the risks of new emerging monopolies. When doing so, take the value of data and the implications of network

effects into account. Remove existing barriers for economic operators trying to enter the DSM. Foster measures that improve data portability and interoperability.

- Regulate dominating search engines, platforms and monopolies by implementing an ex-ante regulatory oversight regime, based on reasonably translating the concept of 'Significant Market Power' to highly dynamic services[5]. Use the thresholds of this concept, where they are more reliable than 'pure' market shares, while avoiding overly difficult definition of markets to ensure swiftly applicable rules. In addition, consider new indicators for market dominance.[6] Regulators should monitor digital markets on an ongoing basis, identify competition problems and bottlenecks, and subsequently impose remedies on companies that abuse their dominant position and engage in anti-competitive behavior.
- Substantially increase the funding and the technical capacity of competition authorities in order to ensure the effective and swift enforcement of competition rules in the fast-paced and complex digital economy. Speed up abuse proceedings and, where necessary, apply interim measures to prevent the negative impact of infringements and avoid markets from tipping while at the same time guaranteeing the procedural defense rights of companies.
- Ensure that merger rules define markets in a realistic way, taking account of global market conditions and adopting a dynamic analysis and long-term view to assess the existence of competitive pressure. In addition, take third country state aid into account.

Taxation: A major problem in the digital economy is the unequal taxation of market participants, a situation that often tends to favor global corporations and non-EU players.

- Address tax optimization strategies based on complex corporate structures that take advantage of tax differences between EU member states by establishing a fair and effective taxation system applicable to all companies offering services in the DSM regardless of their legal form or location. Prioritize a solution at OECD level to avoid fragmentation across Europe. The principle of taxation at the place where a company makes profit and the OECD discussions about 'virtual permanent establishment' seem to indicate a good solution as long as double taxation or additional red tape can be avoided.
- Ensure fair competition for European SMEs with non-EU online sellers by making the recently introduced but so far only optional 'Import One Stop Shop' for VAT collection mandatory. This means requiring all online marketplaces to be liable for VAT obligations of their sellers, thereby preventing VAT fraud.
- Encourage EU member states to address the problem of online retailers that destroy returned or unsold goods by adapting the taxation rules applicable to donations to charitable organizations without holding the donors liable for faulty goods.

Business growth: new and small businesses suffer the most from the unbalanced DSM and often fail to scale up or eventually move to other markets that offer better financial incentives and structural conditions for growing their business.

- Facilitate easy access to public procurement and venture capital for startups and SMEs. Ease the administrative burden for those actors (e.g. by very specific company law additions). Establish an environment in which it is worth for businesses to invest in AI research and other future-oriented technologies (e.g. by providing tax breaks for doing research; an EU-Visa scheme for tech-talents; fast, secure and reliable 5G internet connection; better access to computer capacities and datasets).

[5] Comparable to the German GWB § 19a GWB-RefE.

6 For example, 'Total Consumer Time' as an indicator to show the market power of ecosystems before they monetize their market power and get dominant in the classical sense.

- Better protect European technology startups and key technology knowledge from being sold off by foreign state funds or foreign state-supported cooperation.
- Create the right conditions for more European cooperation to enable our companies and joint ventures to reach the necessary scale and compete worldwide and to promote alternative European systems (e.g. a European Cloud Service). Harmonized European standards in the DSM could be an important approach to achieve this goal and should be further intensified for all digital products, services and processes. Harmonizing civil procedure law is another important means for reducing existing investment obstacles for private investors.
- Conduct a study on the various stock option schemes for startups across Europe: attractive stock options would allow European founders to compete with their US counterparts by selling a share in their idea to high-skilled employees, thereby giving startups in Europe the opportunity to retain talent.

D. ECONOMY

Artificial Intelligence (AI): even though a technology of strategic relevance, most innovation in this field takes place outside Europe which, inter alia, is due to insufficient investments, the lack of big data for algorithm training purposes as well as the uncertainty for companies caused by ongoing discussions about legal and ethical questions.

- Develop a risk-based framework for AI covering high-level ethical standards and appropriate liability rules while at the same time providing the private sector with enough flexibility as well as legal certainty to develop new business models. It is crucial that this set of rules harmonizes the legal situation across Europe. Any legislation should also aim at:
  a) finding the right balance between privacy, security and innovation;
  b) ensuring strong intellectual property rights that offer legal certainty to encourage new innovation;
  c) reviewing if existing horizontal rules such as the GDPR or the product liability directive support or hamper AI innovation. Bearing this legislation in mind, any new AI regulation should avoid over-regulating the new AI market;
  d) avoiding overlaps with other upcoming legislation (e.g. strict conditions for data processing under the e-privacy regulation vs. big data needs for AI-training purposes);
  e) addressing open ethical and legal questions raised by new possibilities based on face and voice recognition;
  f) distinguishing between high-risk and low-risk AI use cases as the definition of AI is constantly evolving. Therefore, legislators should focus on the first category but give businesses the flexibility to choose measures that deliver the best outcomes for the second category;
  g) safeguarding that AI-based decisions do not entail unintentional or hidden negative biases (e.g. refusal of loans or promotions based on gender- or country-biased discrimination).
- Introduce an independent and adequately resourced entity to supervise uniform and EU-wide enforcement of the new legal principles for AI. It should also assist public authorities and businesses in assessing the effects of automated decision-making. In sectors like healthcare or finance, which already feature regulatory agencies, the new entity would have a supportive and coordinating role.
- Accelerate knowledge transfer from research and science to AI applications in industry and the public sector. Establish European AI data centers, jointly developed by government and industry, using strong encryption to protect the stored data in an appropriate manner. Support the development of large-scale testing sites for AI. Provide financial incentives at EU level to launch pilot-projects in Member States.

ANNEX

Platform economy: the increasing importance of platforms raises numerous questions related to governance in the online world by the private sector and on how to handle user-generated content on B2C-platforms. One particular problem in this field are the various national interpretations and definitions of harmful and illegal content.

- Review and harmonize the e-Commerce directive and build on its solid foundation to establish a clear, uniform and up-to-date regulatory framework by taking into account other existing legislation (e.g. the Copyright directive and the Digital Content directive). This process should include a comprehensive consultation on:
  a) The need for clear definitions and more effective rules to fight harmful and illegal content (e.g. harmonized rules for notice and takedown procedures) while preserving the freedom of speech and other fundamental rights;
  b) The different types of proactive measures (e.g. repeating offender policies, the use of trusted flaggers, bulk notification submissions) that can be employed where appropriate by service providers to systemically prevent abuses by users, in particular to tackle the dissemination of such content to the public;
  c) More efficient strategies to protect minors' physical, mental and moral development: digital literacy of parents and their children is key for them to be equipped to face the risks of the online environment;
  d) The growing number of non-EU-based platforms importing products into the EU without respecting EU law on product safety, environmental and consumer protection, labeling or intellectual property;
  e) Any new framework must be manageable for SMEs and start-ups and should therefore include proportionate obligations and clear safeguards for all sectors.

  Online platforms that actively host/moderate content should bear more responsibility for the content they host: a duty-of-care-approach ought to be discussed. This would encourage platform responsibility to proactively prevent illegality (e.g. via a good-Samaritan-principle) rather than focusing solely on direct liability and content removal thereby providing incentives for platforms to stay as passive as possible in order to avoid liability.
- Promote the creation of next generation European platforms based on established standards for consumer and data protection, security and transparency. Especially in the B2B and B2G markets, Europe has enormous potential. European public services could also use these European platforms for their open-data-strategy, allowing them to use a secure, pan-European and interoperable structure.
- Require platforms and service providers without a permanent establishment in the EU to designate a legal representative for consumer interests within the European Union, modelled after the GDPR. The contact information of this representative has to be easily visible and accessible (e.g. via a website or app).[7]
- Conduct a study on the digital anonymity of users and legislative approaches to create a system of trustworthy identity management for social media that enables individuals to express their opinion but at the same time makes them identifiable if they commit a crime.
- Introduce transparency rules for social media platforms to disclose the funding and the power of interest groups behind influencers who use those platforms, thereby making it easier to assess and understand the intentions of those actors. Introduce a 'funded by' disclaimer that shows who is legally responsible for the content, how many people saw it and from which geographic location. Consider the application of press law and the right of objection and correction to social media by adjusting existing legislation (e.g. the Audiovisual Media Services Directive.

[7] See Article 4 Market Surveillance Regulation, which already creates for certain products the obligation for importers from third countries to have a legal representative based in EU territory.

ANNEX

Digital Finance: Distributed ledger technology (DLT), big data and cloud computing have the potential to fundamentally change the financial industry but are currently not regulated and many fundamental policy decisions in this field also remain pending.

- Apply all relevant EU legislation and regulation to all providers of financial services in the Internal Market based on the principle of 'same activity, same risk, same rules, same supervision', regardless of the legal form or the location of the provider. At the same time, allow the concept of regulatory sandboxes for a certain timeframe for new business models in the field of experimental technologies (= hard innovation in the blockchain field).
- Propose legislation to regulate crypto assets and thereby codify that all legal tender has to be recognized by legal systems and has to be supervised by the competent authorities. Evaluate as soon as possible if there is need for a European crypto-currency in close cooperation between the ECB and European banks and in doing so, take the environmental impact of crypto currencies into account. In case of a favorable decision, the EU crypto-currency should not compete with the Euro but should rather be recognized as a valid transaction tender. Such a public system could give the European Union great competitive advantage. Also evaluate if a European payment platform, with high security standards, is necessary to secure valuable data records.
- Create a legal framework for the secure use of DLT like blockchain technology (including lending), cloud computing, big data and AI for financial services as well as trading and make it compatible with the current supervisory regulatory framework. Cooperate closely with the financial sector to improve the resilience of financial systems against cyber-attacks.
- Harmonize e-payment systems and digital authentication, foster crowd-funding while fully implementing the 5th Anti-Money-Laundering directive - add alternatives to existing paper form requirements and other provisions that are not fully technology-neutral.

Infrastructure, sustainability and smart cities: The digitization of cities and infrastructure is making slow progress and does not follow a clear vision on how to use different technologies efficiently and sustainable as well as on how to trigger synergy effects between them. Too often old and uncompetitive technologies are being protected in the market at the disadvantage of innovative technologies.

- Develop a human-centered and ethically sound vision for the European Union on how to use different technologies efficiently and sustainably, in particular for our cities and infrastructures. Invest and cooperate closely with the private sector in order to create lighthouse projects in volunteering cities, where all available state-of-the-art technologies are combined and real-life tests are constantly conducted (including smart buildings, smart grids, connected cars, mobility platforms, public services, and logistics).
- Create new and support existing Digital Innovation Hubs in European regions, which cluster European stakeholders (such as companies, universities, research institutes, start ups, municipalities) and thereby build up innovative ecosystems for new technologies. The hubs should focus on different areas of expertise, based on a strategic approach, which considers the strengths and existing capacities of the specific regions. In order to qualify as a hub, a minimum level of technology and capabilities has to be reached. Regular exchange of insights and experiences should be mandatory. Also introduce the idea of 'Competence Centers' with a focus on SMEs on a European level, as they already exist in some Member States. Exploit synergies between Digital Innovation hubs, competence center, Horizon hubs and EIT hubs.
- Encourage data sharing between different companies in the same supply chain and guarantee that the movement of meta-data between different machines/entities (e.g. cars, road, authorities, lighting, advertisers) takes place in an innovative manner by further strengthening interoperability and by establishing common standards.
- Develop a plan for strategic investments in turning-point technologies like 5G and in digital manufacturing of key industrial sectors with a priority for green growth (e.g. energy

efficiency, raw materials mined free of human-rights violations) in order to achieve a sustainable low-carbon and eventually carbon-free economy.

- Avoid digital gaps between regions by deploying 5G / gigabit networks for all European citizens. However, in the beginning one should focus on all urban areas and major ways of transportation. The proposal of the European Commission to allocate 3 billion Euros in funding for digital infrastructure under the Connecting Europe Facility (CEF) should be considered as a minimum. Prevent fragmentation of 5G spectrum and support the 5G roll-out by ensuring an investment-friendly environment (e.g. by changing construction laws) that allows for fast, non-bureaucratic and cost-efficient network deployment. Enhance EIB support for smaller projects in rural areas. Set up timetables and financial incentives for Member states, cities, regions and industry, accelerate the administrative approval processes and clarify that public procurement and public subsidies are not a hurdle. To increase the 5G demand by citizens in all Member States, introducing a voucher system seems reasonable.

Research in digital technologies: Although Europe has the necessary financial resources for significant research investments in digital technologies, China and the United States are outspending Europe in almost every field, giving them a decisive technological advantage.

- Increase EU investments in the research of key technologies like AI, robotics, quantum computing, microelectronics, batteries, the Internet of Things, nano-technology, DLT and 3D printing. Conduct a study on how to create synergy effects and on how important high-energy consuming technologies can be balanced off by efficiency gains in other areas. Exploit synergies between 'Horizon Europe', the Digital Europe Program and the Connecting Europe Facility (CEF) and do not cut the funding for digital technologies.
- Encourage all Member States to spend a significant part of their GDP on research in digital technologies. The objective should be at least 20-25 billion Euro of public and private investments per year. Continue strengthening the 'European Innovation Council' and expand the 'Digital Europe Program', which is a good starting point but hardly enough to compete with the US and China in the coming years. The allocated total amount of 9.2 billion Euro should thus be considered a minimum and might need to be increased in the course of the ongoing MFF negotiations.
- Create more chairs at European universities and provide more funding for AI and other key technologies in order to properly train the next generation of researchers and entrepreneurs. Pool relevant resources and competences within the EU.
- Improve knowledge transfer between our world class research and the business world, for instance, by setting up business networks, regulatory sandboxes as well as contact points with legal personnel and business consultants in universities.

E. DATA

Data protection: While data protection in Europe has successfully set global standards, it has also proven to be too burdensome and complex in many real-life scenarios.

- Use the GDPR review to revise specific aspects of the law. In my opinion, the following issues are the most pressing:
    a) Allow for new technologies (e.g. Distributed Ledger Technology like blockchain, big data, AI) to use personal data as long as it is in line with fundamental rights. The concept of informed consent has to be updated, at least when it comes to AI and automated learning processes: risk-based approaches might be suitable;
    b) Promote pseudonymized data as a third data category that allows the use of personal data while preserving anonymity;

c) Guarantee the strict enforcement of GDPR in the processing and the commercial use of personal data generated by wearable devices and voice assistants (e.g. in case of personalized advertisements or insurance applications). At the same time, it should be ensured that data can be used, in compliance with GDPR, for the training and development of algorithms. Empower consumers to take informed decisions on the privacy implications of using these new technologies and ensure they have easy-to-use options to delete their personal data as is foreseen in the GDPR;
d) Ensure that profiling based on factors such as income, gender, geographic location and others does not lead to discrimination in price, service quality or availability of offers;
e) Clarify certain articles of the GDPR to avoid differing interpretations (e.g. Art 15, 20, 26, 28);
f) Enhance the uniform implementation of the GDPR across the EU by reducing the opening clauses and by making the consistency mechanism compulsory;
g) Withdraw the e-privacy proposal and include specific parts of it in the GDPR;
h) Create a user-friendly and transparent permission process to reduce the number of interactions between service providers and end-users ('cookie fatigue'), thereby striking a balance between the protection of individual consumers and the secure processing of communications data based on pseudonymised data processing;
i) Include further exceptions for societies, associations and micro enterprises to reduce red tape and introduce better support mechanism for them to apply GDPR provisions;
j) Create a template for binding corporate rules and a code of conduct to help European businesses and to reduce the workload of national data protection authorities;
k) Streamline the enforcement of GDPR and better equip data protection authorities to this end: numerous differing national or even local interpretations[8] of the legal text are currently creating geographical advantages/disadvantages for companies;
l) Offer a standardized and automated way to interact with GDPR decisions via an application programming interface (API);
m) Complement the European Data Protection Board with a board of stakeholders from research, industry, users and consumer organizations, religious associations and civil society organizations;
n) Address the problem that some companies exploit the situation in third countries where GDPR rules do not apply to training their AI or test their new data driven business models without any restrictions and later use these data experiments to successfully capture market share in Europe.

- Develop a legal framework for the Internet of Things by harmonizing existing legislation of different sectors (e.g. product liability directive, radio equipment directive, machinery directive), by removing unnecessary legal obstacles and by including privacy by design as well as security by design solutions.
- Establish a European Digital Identity ecosystem for safe online identification and age verification using only personal data that is strictly necessary for the purpose of the service. In the interest of fast growth of reach and usage and to avoid segmentation, the use of existing and certified systems and services should be promoted. In this context, a mandatory European Single Sign-On Standard should be initiated for digital services and downstream services (e.g. mobile apps and web sites). While using these tokens, the access to data, systems and networks and all internal and external communications must be protected. Correct and secure collection, processing, storing and forwarding of biographical and biometric data must be ensured at any time. In this context, a study is needed to examine how DLT could be used to create a resilient EU Digital Identity system.
- Set up a European cloud system with the support of the public and private sector, combining existing cloud services that comply with our key rules and standards (e.g. cyber security, data

[8] See Germany with its sixteen federal states, each with its own Data Protection Authority.

protection) and is based on interoperability. Instead of replicating non-European hyperscalers, we should create the infrastructure that enables trustworthy cloud providers to cooperate (Europeanizing the Gaia-X project would be one option). Increase the number of common data spaces to incentivize voluntary data-sharing between businesses. Store public non-personal data in a European Cloud system and make it available for all European AI technologies.

Global Data Flows: Certain actors outside the European Union intend to restrict the free flow of data for undemocratic, profit-making or geopolitical reasons, while anti-globalization movements within the European Union aim to reduce global digital trade and minimize international data transfer.

- Cooperate with the G20, OECD and WTO to further develop the free flow of data in trade and non-trade agreements, except where this undermines European interests (e.g. lowering our high data protection standards) or where restrictions are proportionate and justified on certain grounds (e.g. public security). Develop an evidence-based and targeted policy to better tackle barriers to digital trade (e.g. the WTO eCommerce initiative).
- Uphold existing adequacy arrangements, in particular the EU-US Privacy Shield and continue to pursue data adequacy talks with countries like South Korea, India, Australia, Brazil and Chile to promote certifying privacy policies and to allow the exchange of data with third countries.
- Call on the European Data Protection Board to pass guidelines that address the issue of time gaps between the suspension of an existing adequacy arrangement (e.g. Safe Harbor) and the time when a new regime becomes effective. As our daily life depends more and more on international data flows, affected actors such as businesses or universities should be able to continue their work with legal certainty.

F. SOCIETY

eGovernance: In most Member States the digital transformation of public services and administrations is stagnating, which aggravates the bureaucratic burden for citizens and businesses and causes long delays. Two major obstacles are unresolved: liability issues and extensive and sometimes conflicting rules at European, national and regional level that the respective authorities are obliged to follow.

- Renew the 'eGovernment Action Plan' and use it together with the 'Digital Europe Program' as common legal frameworks to support all central public and as many local administrations as possible to fully adopt digital technologies (based on AI, Big Data applications and DLT like blockchain), wherever beneficial and feasible and in line with the European Open-Source Strategy. The objective should be to increase the usage of eGovernment services by up to 70-80% of all EU-citizens over the next five years. In addition and in order to establish a secure digital identity, the possibility of subsequent authentication and the principle of Single Sign-on standards are of decisive importance for this initiative.
- Speed up the implementation of the Digital Single Gateway and promote the development of interoperable platforms that offer cross-border services in the European Union, while meeting common security standards for all services in all Member States. Encourage better cooperation between federal and local authorities on topics such as mobility, environment and climate change targets.
- Update and expand the eIDAS regulation and make the use of services for secure digital identities more binding. Use the forthcoming eIDAS-evaluation to introduce an eID function for legal entities and an interoperable identity standard for e-governance services. In parallel, authorities must be stimulated to reduce the use of paper, to stick to the 'once-only-principle' and to offer e-translation services.

- Establish a holistic EU-classified network to further enhance inter-agency collaboration for sensitive matters as the need for the exchange of classified information between EU-government entities for security or military purposes increases constantly.

e-Health: Although innovative technologies could significantly improve the identification of health risks, help developing more effective drugs and lead to higher quality in treatments as well as of healthcare in remote regions, the digital transformation in health has so far often been restricted to new devices.

- Create the legal and technological basis for a European Digital Health Ledger: this system should protect individual information by not identifying the respective person while at the same time improve the quality of available data for each European citizen by allowing digital tools to work properly (e.g. based on self-learning algorithms or big data analysis). The data of this system should be stored in anonymized form in Open Data Trust Centers and should be available for further research as well as the development of new drugs and treatments. Support existing national initiatives to foster the availability of health data.
- Further develop the legal framework for online medical consultation and promote the interconnectivity between European health entities by using international accepted standards (e.g. FHIR, SNOMED) in order to facilitate best practices and evidence-based treatments.
- Conduct a study to assess the need for regulation in this area and to examine how self-learning algorithms, AI, big data tools and robotics can support our health systems in practice to further enhance the quality of health care and to evaluate the potential risks of those technologies. The objective should be to provide the involved actors (e.g. doctors, hospitals, health companies) with all necessary personal health data without identifying a specific patient. Make sure that AI applications are not biased or have blind spots (e.g. heart attacks in women are often under-diagnosed and miss-treated as most of the research is done on men).

Employment, education and digital skills: Our concepts of learning and working are still too defined by the job market needs of a pre-digital world, which leads to a growing skills gap. At the same time, digital ways of making processes in this area more efficient and of improving the work-life-balance are not yet sufficiently applied. Vast differences between Member States also intensify the trend of job market polarization in certain regions.

- Promote the introduction of mandatory digital and computational skills courses in all European schools, universities and educational institutions. Make sure that students develop a sound knowledge of cyber protection methods, AI, data analysis, data assessment and digital privacy. Encourage the inclusion of 'digital literacy' in school curricula to ensure that every student is taught how to develop critical as well as creative thinking skills and digital resilience. A focus should be on the ability to detect and deal with misinformation. Pathways towards additional education to specialize in AI (e.g. master and PhD degrees, part-time study) should also be offered.
- Promote and increase the funding for STEM (Science, Technology, Engineering and Mathematics) academic disciplines to increase the number of students in these fields while considering the unbalanced gender situation, which might create gender disadvantages in the future.
- Cooperate with the private sector to promote the concept of lifelong learning and to introduce digital skills trainings across Europe in order to teach employees of all generations and all forms of employment how to use digital technologies. Develop policies for the re-skilling and up-skilling of the workforce with a focus on digital manufacturing. Draw on existing public-private cooperation initiatives (e.g. Forum for Digital Resilience) to provide for a regular solutions-oriented policy dialogue and to contribute to the planned 'EU Digital Education Action Plan'.

ANNEX

- Conduct studies and discuss their findings on:
  a) The most effective models to improve digital literacy in Europe, based on examples and experiences from various Member States;
  b) How we should rethink our work processes and business models (e.g. offering flexible working models that can be tailored to an individual lifestyle). Short-term-employment contracts with companies in different Member States on a 'digital home office' base should not lead to gaps in pensions and unemployment benefits. Overall, we should promote good practices of corporate cultures, collective agreements and national legislation that aim to promote a healthy work-life balance and working time in the digital economy on the basis of our common European standards;
  c) What is the impact of digitization on our traditional social welfare systems and how do we need to adapt our labor laws to the new realities? To this end, the European Commission should explore to what extent already existing EU legislation, notably the Directive on Temporary Agency Work, is applicable to certain online platforms.

Media and culture: Digitization has changed the way we receive and consume news as well as how they are amplified when distributed. This has made the media landscape much more pluralistic but also more vulnerable to disinformation, to an overkill of information and prone to the influence of a few dominating actors.

- Introduce legislation to address the problem of disinformation and complement the voluntary measures taken in the context of the 2018 'EC Code of Practice against Disinformation', which covers the advertising industry and online platforms. Legislation must take the evolutionary nature of the issue into account and foster cooperation between platforms and traditional media.
- Create a European Media Watch Centre to systematically examine possible disinformation sources and to counter adverse propaganda. Moreover, develop and conduct specific trainings for journalists on the detection of disinformation and create a taskforce to improve information sharing among media actors. Promote the introduction of similar trainings to improve digital media literacy for the general public starting in schools.
- Prepare an ambitious Media Action Plan, to be based on an in-depth study of the European media landscape and a public consultation. The plan should focus on creating an enabling framework for the media to thrive, by ensuring better coordination in policy-making and identifying key themes of interest (e.g. media freedom, sustainability and fair competition). In addition, conduct a study on how to promote media pluralism and freedom in a digital world and examine new business models.
- Ensure that the level-playing field provisions introduced in the AVMSD for media companies and online platforms are timely implemented by all EU Member States. Similar legal obligation on access to digital advertising markets will be key. Timely implementation also helps to ensure better cross-border access for language minorities and citizens of border regions to audiovisual works.
- Foster European productions and continue to push for EU narratives and stories in existing cooperation with non-European networks and providers. Preserve Europe's cultural heritage digitally (including libraries, archives, museums and buildings records).